Contoso: Full Scan-Vulnerability Trend Report

Report Generated: January 7, 2022

1 Introduction

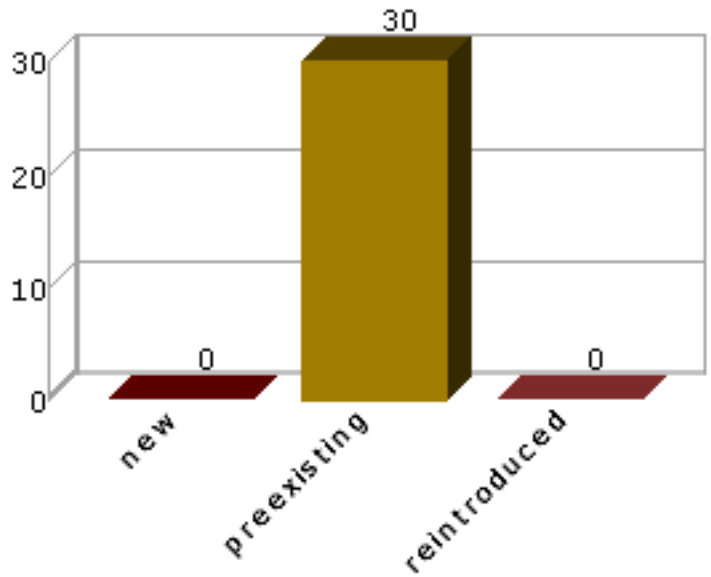
On January 7, 2022, at 1:15 AM, a heavy vulnerability assessment was conducted using the SAINT 9.9 vulnerability scanner. The scan discovered a total of one live host, and detected zero critical problems, four areas of concern, and 26 potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

2 Summary

The sections below summarize the results of the scan.

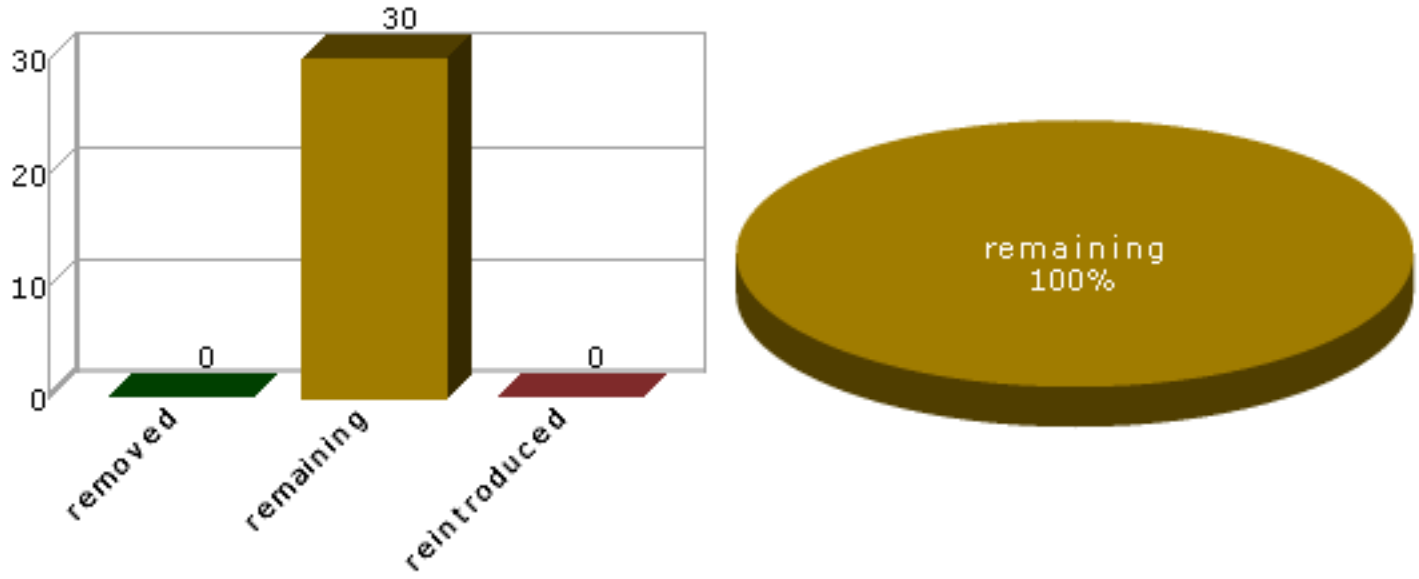
2.1 Status of Current Vulnerabilities

Includes critical problems, areas of concern, and potential problems.



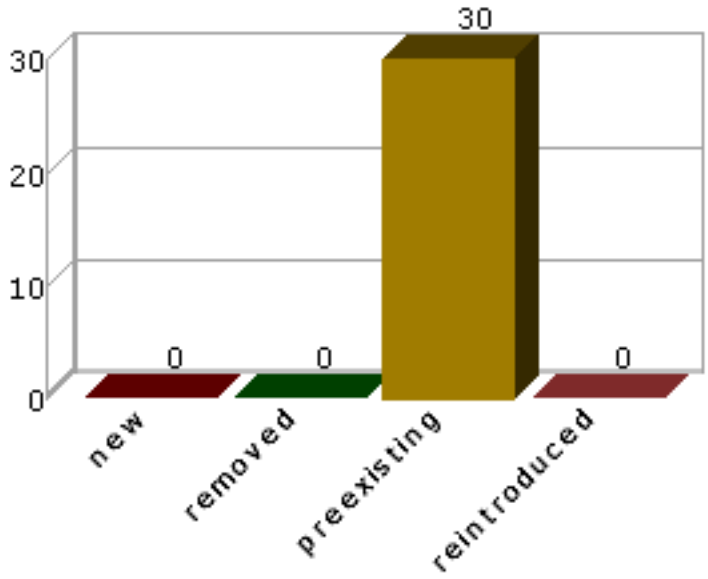
2.2 Status of Old Vulnerabilities

Includes critical problems, areas of concern, and potential problems.

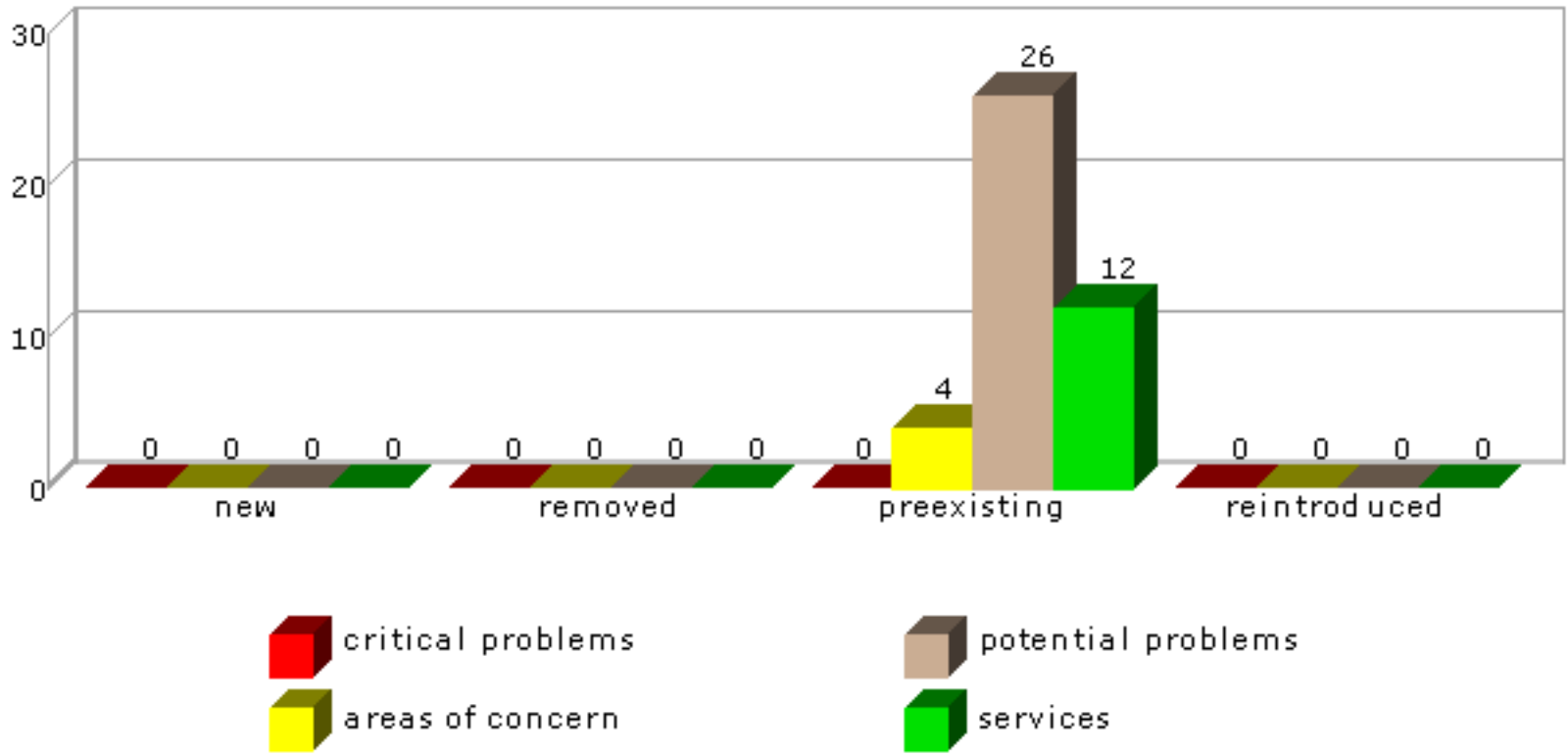


2.3 Status of All Vulnerabilities

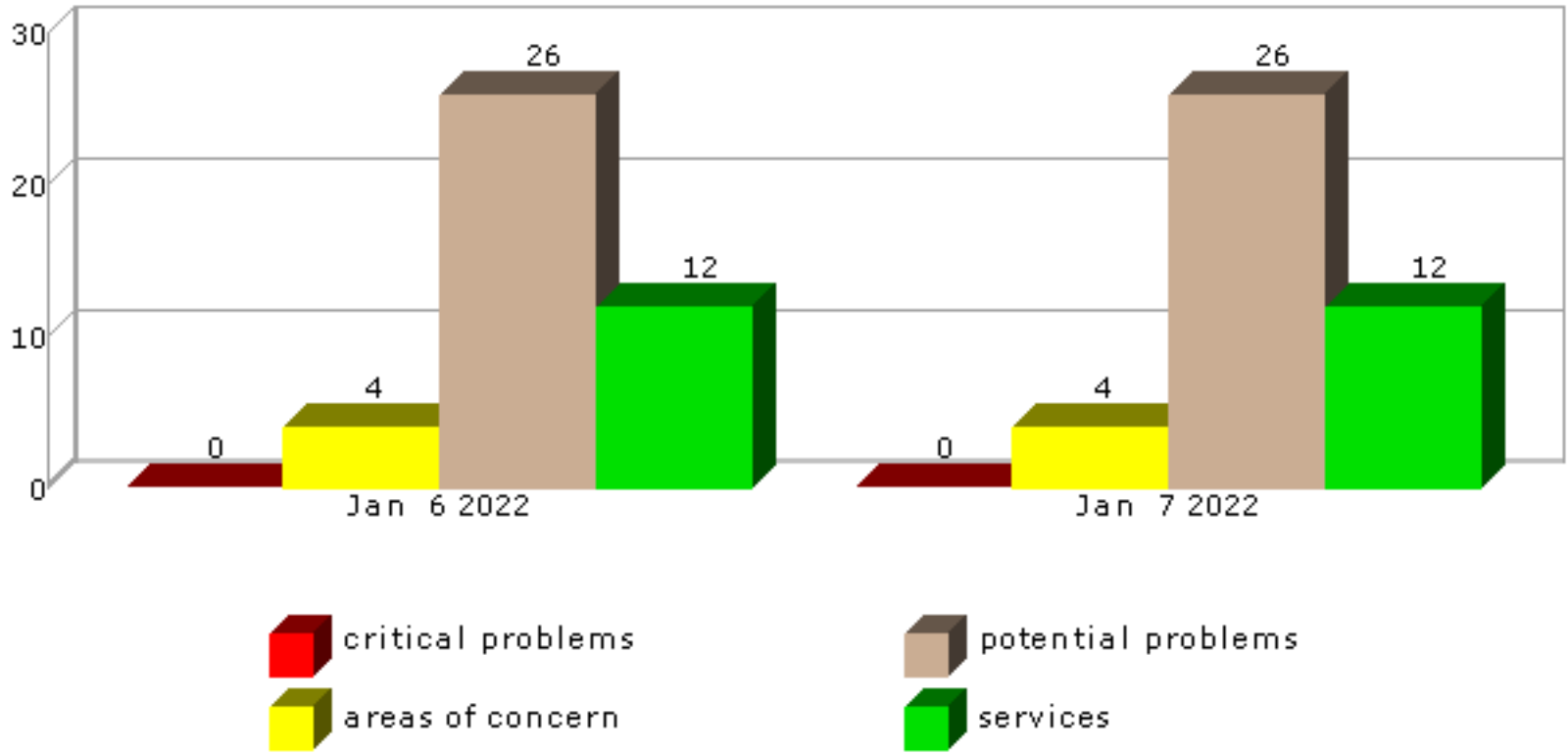
Includes critical problems, areas of concern, and potential problems.



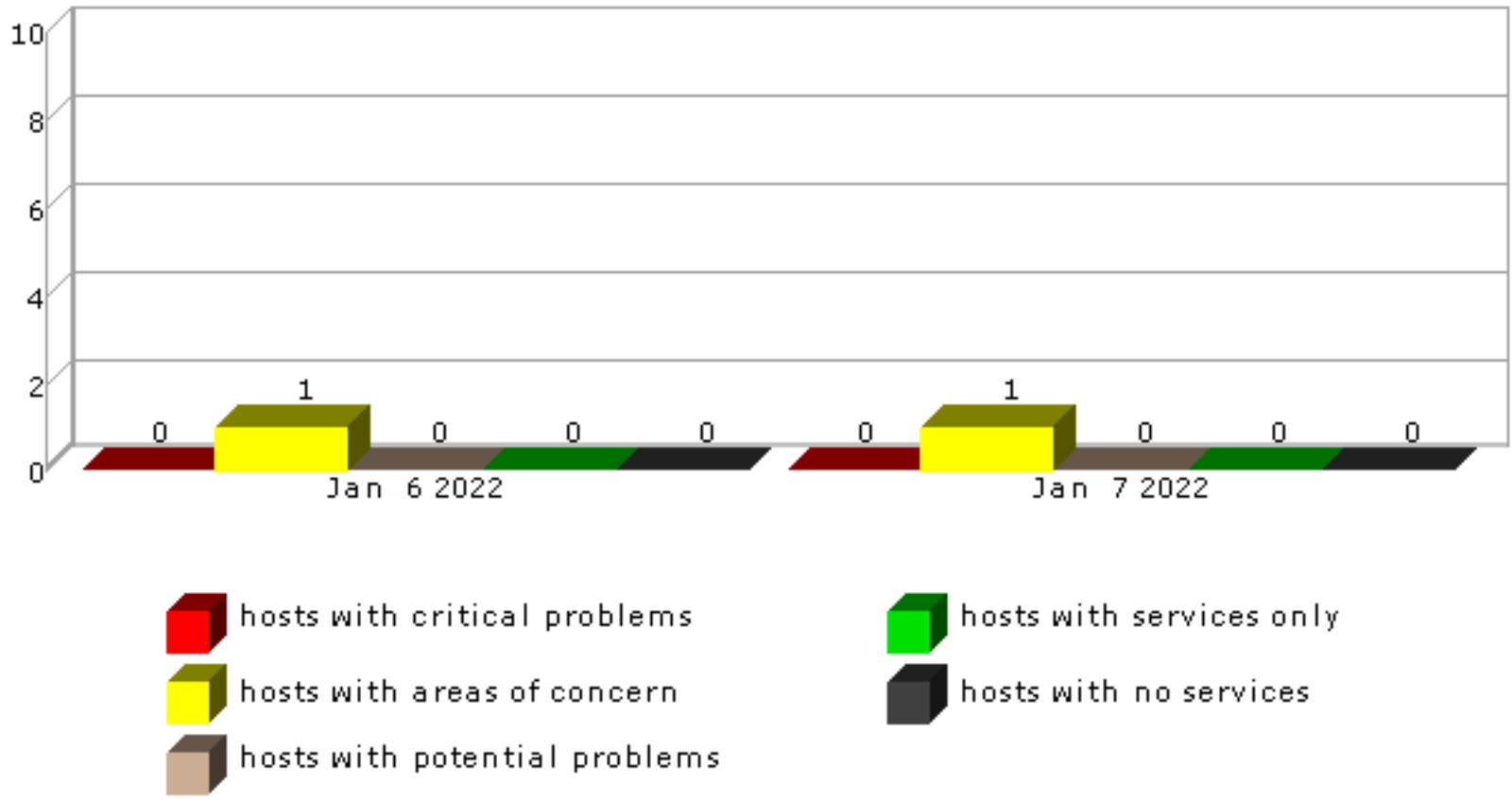
2.4 Vulnerability Status by Severity



2.5 Vulnerability History



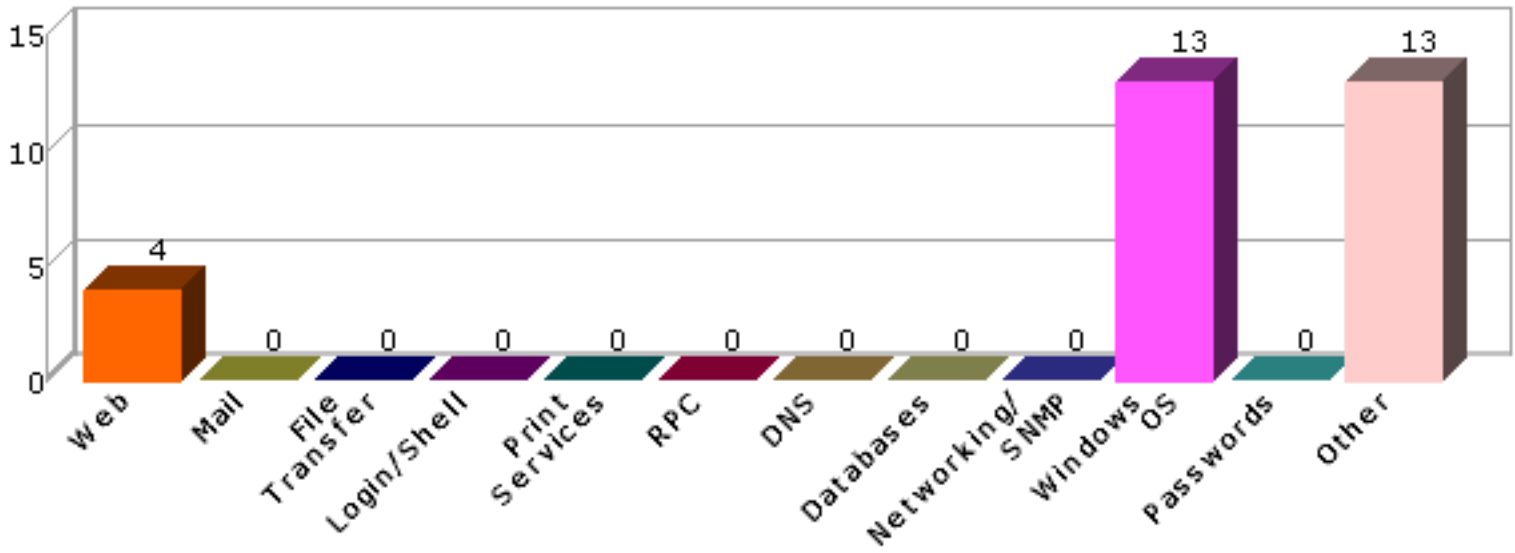
2.6 Host History

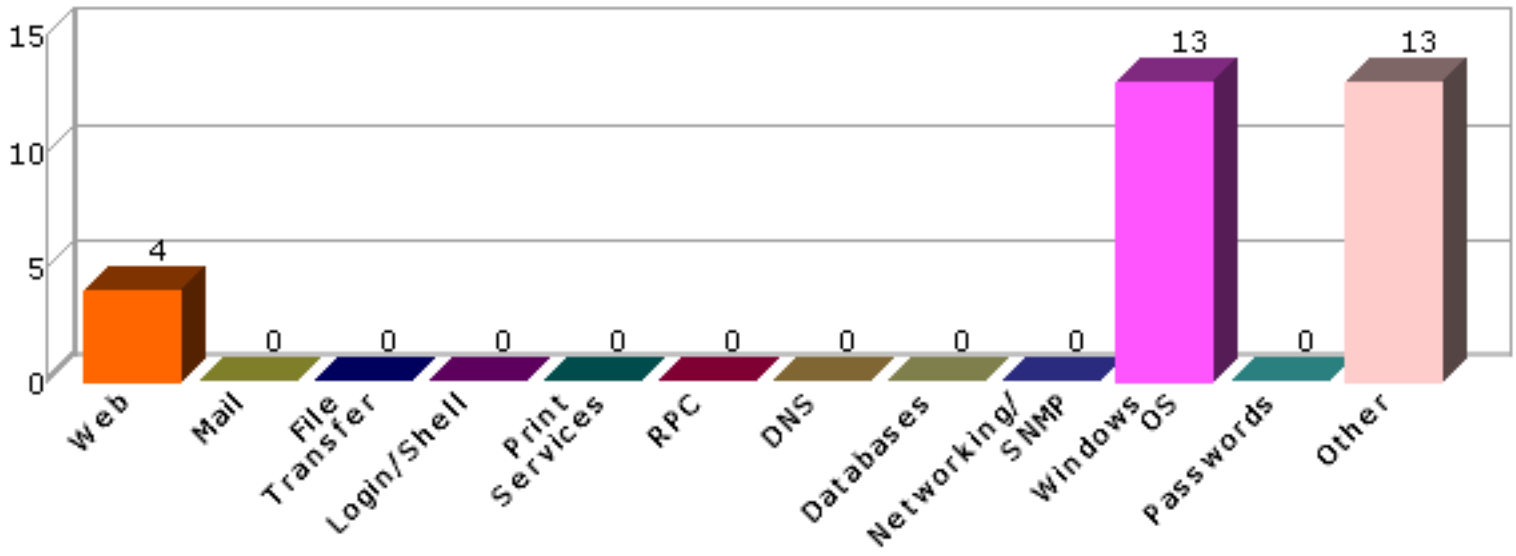


2.7 History of Vulnerabilities by Class

This section shows the number of vulnerabilities detected per scan in each vulnerability class.

Jan 6 2022





3 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

3.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems	Status
contoso-svr1.contoso.local		10.101.5.2	Windows Server 2016	0	4	26	preexisting

3.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Port	Severity	Vulnerability / Service	Status	CVE	Max. CVSSv2 Base Score

contoso-svr1.contoso.local	139 /tcp	concern	vulnerable JRE version: 1.8.0_131	preexisting	CVE-2016-10165 CVE-2016-9840 CVE-2016-9841 CVE-2016-9842 CVE-2016-9843 CVE-2017-10053 CVE-2017-10067 CVE-2017-10074 CVE-2017-10078 CVE-2017-10081 CVE-2017-10086 CVE-2017-10087 CVE-2017-10089 CVE-2017-10090 CVE-2017-10096 CVE-2017-10101 CVE-2017-10102 CVE-2017-10105 CVE-2017-10107 CVE-2017-10108 CVE-2017-10109 CVE-2017-10110 CVE-2017-10111 CVE-2017-10114 CVE-2017-10115 CVE-2017-10116 CVE-2017-10118 CVE-2017-10125 CVE-2017-10135 CVE-2017-10176 CVE-2017-10193 CVE-2017-10198 CVE-2017-10243 CVE-2017-10274 CVE-2017-10281 CVE-2017-10285 CVE-2017-10293 CVE-2017-10295 CVE-2017-10309 CVE-2017-10345 CVE-2017-10346 CVE-2017-10347 CVE-2017-10348 CVE-2017-10349 CVE-2017-10350 CVE-2017-10355 CVE-2017-10356 CVE-2017-10357 CVE-2017-10388 CVE-2018-11212 CVE-2018-13785 CVE-2018-2579 CVE-2018-2581 CVE-2018-2582 CVE-2018-2588 CVE-2018-2599 CVE-2018-2602 CVE-2018-2603 CVE-2018-2618 CVE-2018-2627 CVE-2018-2629 CVE-2018-2633 CVE-2018-2634 CVE-2018-2637 CVE-2018-2638 CVE-2018-2639 CVE-2018-2641 CVE-2018-2663 CVE-2018-2677 CVE-2018-2678 CVE-2018-2783 CVE-2018-2790 CVE-2018-2794 CVE-2018-2795 CVE-2018-2796 CVE-2018-2797 CVE-2018-2798 CVE-2018-2799 CVE-2018-2800 CVE-2018-2811 CVE-2018-2814 CVE-2018-2815 CVE-2018-2938 CVE-2018-2940 CVE-2018-2941 CVE-2018-2942 CVE-2018-2952 CVE-2018-2964 CVE-2018-2973 CVE-2018-3136 CVE-2018-3139 CVE-2018-3149 CVE-2018-3169 CVE-2018-3180 CVE-2018-3183 CVE-2018-3209 CVE-2018-3211 CVE-2018-3214 CVE-2019-11068 CVE-2019-13117 CVE-2019-13118 CVE-2019-16168 CVE-2019-18197 CVE-2019-2422 CVE-2019-2426 CVE-2019-2449 CVE-2019-2602 CVE-2019-2684 CVE-2019-2697 CVE-2019-2698 CVE-2019-2699 CVE-2019-2745 CVE-2019-2762 CVE-2019-2766 CVE-2019-2769 CVE-2019-2786 CVE-2019-2816 CVE-2019-2842 CVE-2019-2894 CVE-2019-2933 CVE-2019-2945 CVE-2019-2949 CVE-2019-2958 CVE-2019-2962 CVE-2019-2964 CVE-2019-2973 CVE-2019-2975 CVE-2019-2978 CVE-2019-2981 CVE-2019-2983 CVE-2019-2988 CVE-2019-2989 CVE-2019-2992 CVE-2019-2996 CVE-2019-2999 CVE-2019-6129 CVE-2019-7317 CVE-2020-14556

CVE-2020-14577 CVE-2020-14578 CVE-2020-14579 CVE-2020-14581 CVE-2020-14583 CVE-2020-14593 CVE-2020-14621 CVE-2020-14664 CVE-2020-14779 CVE-2020-14781 CVE-2020-14782 CVE-2020-14792 CVE-2020-14796 CVE-2020-14797 CVE-2020-14798 CVE-2020-2583 CVE-2020-2585 CVE-2020-2590 CVE-2020-2593 CVE-2020-2601 CVE-2020-2604 CVE-2020-2654 CVE-2020-2659 CVE-2020-2754 CVE-2020-2755 CVE-2020-2756 CVE-2020-2757 CVE-2020-2773 CVE-2020-2781 CVE-2020-2800 CVE-2020-2803 CVE-2020-2805 CVE-2020-2830	7.5

contoso-svr1.contoso.local	139 /tcp	concern	vulnerable Mozilla Firefox version: 62.0.3	preexisting	CVE-2018-12388 CVE-2018-12390 CVE-2018-12392 CVE-2018-12393 CVE-2018-12395 CVE-2018-12396 CVE-2018-12397 CVE-2018-12398 CVE-2018-12399 CVE-2018-12401 CVE-2018-12402 CVE-2018-12403 CVE-2018-12405 CVE-2018-12406 CVE-2018-12407 CVE-2018-17466 CVE-2018-18356 CVE-2018-18492 CVE-2018-18493 CVE-2018-18494 CVE-2018-18495 CVE-2018-18496 CVE-2018-18497 CVE-2018-18498 CVE-2018-18500 CVE-2018-18501 CVE-2018-18502 CVE-2018-18503 CVE-2018-18504 CVE-2018-18505 CVE-2018-18506 CVE-2018-18510 CVE-2018-18511 CVE-2018-6156 CVE-2019-11691 CVE-2019-11692 CVE-2019-11693 CVE-2019-11694 CVE-2019-11695 CVE-2019-11696 CVE-2019-11697 CVE-2019-11698 CVE-2019-11699 CVE-2019-11700 CVE-2019-11701 CVE-2019-11702 CVE-2019-11707 CVE-2019-11708 CVE-2019-11709 CVE-2019-11710 CVE-2019-11711 CVE-2019-11712 CVE-2019-11713 CVE-2019-11714 CVE-2019-11715 CVE-2019-11716 CVE-2019-11717 CVE-2019-11718 CVE-2019-11719 CVE-2019-11720 CVE-2019-11721 CVE-2019-11723 CVE-2019-11724 CVE-2019-11725 CVE-2019-11727 CVE-2019-11728 CVE-2019-11729 CVE-2019-11730 CVE-2019-11733 CVE-2019-11734 CVE-2019-11735 CVE-2019-11736 CVE-2019-11737 CVE-2019-11738 CVE-2019-11740 CVE-2019-11741 CVE-2019-11742 CVE-2019-11743 CVE-2019-11744 CVE-2019-11745 CVE-2019-11746 CVE-2019-11747 CVE-2019-11748 CVE-2019-11749 CVE-2019-11750 CVE-2019-11751 CVE-2019-11752 CVE-2019-11753 CVE-2019-11754 CVE-2019-11757 CVE-2019-11758 CVE-2019-11759 CVE-2019-11760 CVE-2019-11761 CVE-2019-11762 CVE-2019-11763 CVE-2019-11764 CVE-2019-11765 CVE-2019-13722 CVE-2019-15903 CVE-2019-17000 CVE-2019-17002 CVE-2019-17005 CVE-2019-17008 CVE-2019-17009 CVE-2019-17010 CVE-2019-17011 CVE-2019-17012 CVE-2019-17015 CVE-2019-17016 CVE-2019-17017 CVE-2019-17018 CVE-2019-17019 CVE-2019-17020 CVE-2019-17021 CVE-2019-17022 CVE-2019-17023 CVE-2019-17024 CVE-2019-17025 CVE-2019-17026 CVE-2019-20503 CVE-2019-5785 CVE-2019-5849 CVE-2019-7317 CVE-2019-9788 CVE-2019-9789 CVE-2019-9790 CVE-2019-9791 CVE-2019-9792 CVE-2019-9793 CVE-2019-9794 CVE-2019-9795 CVE-2019-9796 CVE-2019-9797 CVE-2019-9798 CVE-2019-9799 CVE-2019-9800 CVE-2019-9801

					CVE-2019-9802 CVE-2019-9803 CVE-2019-9805 CVE-2019-9806 CVE-2019-9807 CVE-2019-9808 CVE-2019-9809 CVE-2019-9810 CVE-2019-9811 CVE-2019-9812 CVE-2019-9813 CVE-2019-9814 CVE-2019-9815 CVE-2019-9816 CVE-2019-9817 CVE-2019-9818 CVE-2019-9819 CVE-2019-9820 CVE-2019-9821 CVE-2020-12387 CVE-2020-12388 CVE-2020-12389 CVE-2020-12392 CVE-2020-12393 CVE-2020-12395 CVE-2020-12399 CVE-2020-12405 CVE-2020-12406 CVE-2020-12410 CVE-2020-12417 CVE-2020-12418 CVE-2020-12419 CVE-2020-12420 CVE-2020-12421 CVE-2020-15649 CVE-2020-15650 CVE-2020-15652 CVE-2020-15659 CVE-2020-15663 CVE-2020-15664 CVE-2020-15669 CVE-2020-15673 CVE-2020-15676 CVE-2020-15677 CVE-2020-15678 CVE-2020-15683 CVE-2020-15969 CVE-2020-16012 CVE-2020-26950 CVE-2020-26951 CVE-2020-26953 CVE-2020-26956 CVE-2020-26958 CVE-2020-26959 CVE-2020-26960 CVE-2020-26961 CVE-2020-26965 CVE-2020-26966 CVE-2020-26968 CVE-2020-6463 CVE-2020-6514 CVE-2020-6796 CVE-2020-6798 CVE-2020-6799 CVE-2020-6800 CVE-2020-6801 CVE-2020-6805 CVE-2020-6806 CVE-2020-6807 CVE-2020-6811 CVE-2020-6812 CVE-2020-6814 CVE-2020-6819 CVE-2020-6820 CVE-2020-6821 CVE-2020-6822 CVE-2020-6825 CVE-2020-6827 CVE-2020-6828 CVE-2020-6831	10.0
contoso-svr1.contoso.local	139 /tcp	concern	Windows PowerShellGet vulnerable version dated 2016-7-16	preexisting	CVE-2020-16886	7.2
contoso-svr1.contoso.local	139 /tcp	concern	Microsoft Windows Defender MpCmdRun.exe vulnerable version 4.10.14393.4283	preexisting	CVE-2020-1163 CVE-2020-1170 CVE-2020-1461	7.2
contoso-svr1.contoso.local	139 /tcp	potential	AV Information: AntiVirus software not found (AVG F-Secure Forefront Kaspersky McAfee Symantec TrendMicro VIPRE)	preexisting		2.6
contoso-svr1.contoso.local	3389 /tcp	potential	server is susceptible to BEAST attack	preexisting	CVE-2011-3389	4.3
contoso-svr1.contoso.local	139 /tcp	potential	Potentially sensitive information found in CC.txt (D:/CC.txt)	preexisting		2.6
contoso-svr1.contoso.local	139 /tcp	potential	Potentially sensitive information found in Creditcards.txt (D: /Creditcards.txt)	preexisting		2.6

contoso-svr1.contoso.local	139 /tcp	potential	Potentially sensitive information found in cmath_testcases.txt (C: /Python27/Lib/test /cmath_testcases.txt)	preexisting		2.6
contoso-svr1.contoso.local	139 /tcp	potential	Potentially sensitive information found in formatfloat_testcases.txt (C:/Python27/Lib/test /formatfloat_testcases.txt)	preexisting		2.6
contoso-svr1.contoso.local	139 /tcp	potential	Potentially sensitive information found in math_testcases.txt (C: /Python27/Lib/test /math_testcases.txt)	preexisting		2.6
contoso-svr1.contoso.local	139 /tcp	potential	Potentially sensitive information found in msg_25.txt (C:/Python27 /Lib/email/test/data /msg_25.txt)	preexisting		2.6
contoso-svr1.contoso.local		potential	ICMP timestamp requests enabled	preexisting	CVE-1999-0524	0.0
contoso-svr1.contoso.local	139 /tcp	potential	ICMP redirects are allowed	preexisting		2.6
contoso-svr1.contoso.local	139 /tcp	potential	Internet Explorer Shell.Explorer object enabled	preexisting		2.6
contoso-svr1.contoso.local	139 /tcp	potential	last user name shown in login box	preexisting	CVE-1999-0592	10.0
contoso-svr1.contoso.local	139 /tcp	potential	SMB1 protocol is enabled	preexisting		2.6
contoso-svr1.contoso.local	139 /tcp	potential	SMB digital signing is disabled	preexisting		2.6
contoso-svr1.contoso.local	3389 /tcp	potential	SSL/TLS server supports short block sizes (SWEET32 attack)	preexisting	CVE-2016-2183	5.0
contoso-svr1.contoso.local	3389 /tcp	potential	TCP timestamp requests enabled	preexisting		2.6
contoso-svr1.contoso.local	3389 /tcp	potential	Server supports TLS 1.0 protocol	preexisting		2.6
contoso-svr1.contoso.local	8080 /tcp	potential	Web server default page detected	preexisting		2.6
contoso-svr1.contoso.local	80/tcp	potential	Web server default page detected	preexisting		2.6
contoso-svr1.contoso.local	139 /tcp	potential	weak account lockout policy (5)	preexisting	CVE-1999-0582	5.0
contoso-svr1.contoso.local	139 /tcp	potential	weak maximum password age policy (90 days)	preexisting	CVE-1999-0535	10.0
contoso-svr1.contoso.local	139 /tcp	potential	weak minimum password age policy (0 days)	preexisting	CVE-1999-0535	10.0
contoso-svr1.contoso.local	139 /tcp	potential	Windows administrator account not renamed	preexisting	CVE-1999-0585	2.1
contoso-svr1.contoso.local	139 /tcp	potential	Windows guest account not renamed	preexisting		0.9
contoso-svr1.contoso.local	139 /tcp	potential	Password never expires for user Bharti.s	preexisting		0.9
contoso-svr1.contoso.local	139 /tcp	potential	Password never expires for user etadmin	preexisting		0.9

4 Details

The following sections provide details on the specific vulnerabilities detected on each host.

4.1 AntiVirus Information

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

References

For additional information about viruses and anti-virus products, see Virus Bulletin.

4.2 Browser Exploit against SSL TLS

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

Most browser vendors have released updates which prevent this attack, but some affected browsers still remain at this time, so it is still advisable also to fix the problem on the server side. SSLv3 and TLS 1.0 should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file. (The -TLSv1 argument requires Apache 2.2.24 or higher or an update from your Linux vendor.)

```
SSLProtocol all -SSLv2 -SSLv3 -TLSv1
```

- **IIS:** See KB245030 and KB187498.
- **Other:** Consult the web server documentation.

Note that disabling SSLv3 and TLS 1.0 entirely on the server may affect the usability of the web site, as some web browsers may not yet support TLS 1.1.

References

Thai Duong wrote a detailed blog post about this attack, including a video demonstration.
Adam Langley wrote a helpful blog post that helps highlight concerns for both browser vendors and website hosts.
Rob VanderBrink of SANS Internet Storm Center posted a blog update detailing TLS 1.1/1.2 support in many common browsers as of September, 2011.

Eric Rescorla wrote a detailed blog post explaining how the attack works in detail and analyzing the security impact of this vulnerability.

4.3 File content checks

Impact

Sensitive information may be at risk of exposure.

Resolution

Consider encrypting sensitive information.

4.4 ICMP information disclosure

Impact

A remote attacker could obtain sensitive information about the network.

Resolution

Configure the system or firewall not to allow ICMP timestamp requests (message type 13) or ICMP netmask requests (message type 17). Instructions for doing this on specific platforms are as follows:

Windows:
Block these message types using the Windows firewall as described in Microsoft TechNet.

Linux:
Use ipchains or iptables to filter ICMP netmask requests using the command:

```
ipchains -A input -p icmp --icmp-type address-mask-request -j DROP
```

Use ipchains or iptables to filter ICMP timestamp requests using the commands:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

To ensure that this change persists after the system reboots, put the above command into the system's boot-up script (typically **`/etc/rc.local`**).

Cisco:
Block ICMP message types 13 and 17 as follows:

```
deny icmp any any 13
deny icmp any any 17
```

References

For more information about ICMP, see RFC792.

4.5 ICMP redirects

Impact

An attacker could change the routing of packets from the target such that transmitted data could potentially be monitored or modified.

Resolution

Disable ICMP redirects. On Windows, this is done by setting the following registry value:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Name: EnableICMPRedirect
Type: REG_DWORD
Data: 0
```

To disable ICMP redirects on Linux, use the following commands:

```
sysctl -w net.ipv4.conf.all.accept_redirects=0
sysctl -w net.ipv4.conf.all.secure_redirects=0
```

To make the above settings permanent, also set the following lines in the **`/etc/sysctl.conf`** file:

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
```

References

For more information about ICMP redirects, see Ask Ubuntu and Windows Reference.

For more information on securing the Linux kernel, see Linux Kernel /etc/sysctl.conf Security Hardening.

4.6 Internet Explorer vulnerabilities

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

Install the latest cumulative patch for your version of Internet Explorer from the Microsoft Security Update Guide. (Note: you need to "Accept" Microsoft's terms of service in order to see the latest patch).

Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088).

Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864.

Install the update referenced in Microsoft Security Bulletin 05-037 to disable the Javaprxy.dll object.

Disable the ADODB.Stream object as instructed in Microsoft Knowledge Base Article 870669.

Disable the Shell.Explorer object by setting the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type dword, radix hex)
```

To mitigate the impact of the ActiveX instantiation heap memory corruption, set the kill bit for the following CLSIDs:

- `3BC4F3A3-652A-11D1-B4D4-00C04FC2DB8D`
- `4682C82A-B2FF-11D0-95A8-00A0C92B77A9`
- `8E71888A-423F-11D2-876E-00A0C9082467`
- `E2E9CAE6-1E7B-4B8E-BABD-E9BF6292AC29`

- 233A9694-667E-11D1-9DFB-006097D50408
- BE4191FB-59EF-4825-AEFC-109727951E42
- 6E3197A3-BBC3-11D4-84C0-00C04F7A06E5
- 606EF130-9852-11D3-97C6-0060084856D4
- F849164D-9863-11D3-97C6-0060084856D4

To fix the `ADODB.connection` vulnerability, install the fix at MS07-009. or mitigate the impact by setting the kill bit for the following CLSID: 00000514-0000-0010-8000-00AA006D2EA4.

References

For the latest security update release, see the MSRC blog.

For more information on all Internet Explorer security fixes, see the Microsoft Security Update Guide.

The Internet Explorer vulnerabilities patched by Microsoft in September 2017 were reported in The Cumulative security update for Internet Explorer: September 12 2017.

The Cumulative security update for Internet Explorer: August 8 2017.

The Cumulative security update for Internet Explorer: July 11 2017.

The Internet Explorer memory corruption vulnerability was reported in Microsoft Advisory CVE-2017-0201.

The scripting engine memory corruption vulnerability was reported in Microsoft Advisory CVE-2017-0202.

The cross-domain privilege elevation vulnerability was reported in Microsoft Advisory CVE-2017-0210.

The same-origin policy bypass vulnerability was reported in SecurityTracker Alert 1031689.

The Internet Explorer remote code execution vulnerability was reported in Microsoft Security Advisory (2963983).

The `CMarkup` Use-After-Free vulnerability was reported in Secunia Advisory SA56974.

The Security Zone Bypass vulnerability (CVE-2010-0255) was reported in Microsoft Security Advisory (980088).

The CSS parser vulnerability (CVE-2010-3971) was reported in Microsoft Security Advisory (2488013).

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, 11-081, 11-099, 12-010, 12-023, 12-037, 12-044, 12-052, 12-063, 12-071, 12-077, 13-008, 13-009, 13-010, 13-021, 13-028, 13-037, 13-038, 13-047, 13-055, 13-059, 13-069, 13-080, 13-088, 13-097, 14-010, 14-012, 14-018, 14-021, 14-029, 14-035, 14-037, 14-051, 14-052, 14-056, 14-065, 14-080, 15-009, 15-018, 15-032, 15-043, 15-056, 15-065, 15-079, 15-093, 15-094, 15-106, 15-112, 15-124, 16-001, 16-009, 16-023, 16-037, 16-051, 16-063, 16-084, 16-095, 16-104, 16-118, 16-142, 16-144, and 17-006.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

The `setRequestHeader()` related vulnerabilities were reported in Secunia Advisory SA29453.

The URL handling vulnerability in IE7 was reported in Microsoft Security Advisory 943521 and Secunia Advisory SA27007.

The document.open spoofing vulnerability was reported in Secunia Advisory SA26069.

More information on the race condition building DOM objects vulnerability was reported in Secunia Advisory SA25564.

More information on the WPAD proxy server interception vulnerability was reported in NIST Vulnerability Database (CVE-2007-1692).

More information on the `navcancl.htm` cross-site scripting vulnerability may be found at BugTraq ID 22966 and Secunia Advisory SA24535.

More information on the Unload JavaScript vulnerabilities may be found at Bugtraq ID 22678 and Bugtraq ID 22680.

More information on the DirectAnimation ActiveX remote integer overflow may be found at XSec Security Advisory XSec-06-10.

More information on the ActiveX instantiation heap memory corruption may be found at XSec Security Advisories: XSec-06-02, XSec-06-03, XSec-06-04, XSec-06-06, XSec-06-08.

More information on the IsComponentInstalled buffer overflow may be found in Bugtraq ID 16870.

More information on the Stack overflow vulnerability may be found in Bugtraq ID 16687.

Information on the createTextRange vulnerability may be found in Bugtraq ID 17196.

More information on the object tag, modal dialog, and information disclosure vulnerabilities may be found in Bugtraq ID 17658, Bugtraq ID 17713, and Bugtraq ID 17717.

More information on the VML buffer overflow may be found in Bugtraq ID 20096.

The ADODB.Stream object vulnerability was reported in US-CERT alert 04-184A.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in BugTraq ID 16352 and BugTraq.

The three vulnerabilities which are exploited by the Download.Ject trojan were reported in Bugtraq ID 10472, Bugtraq ID 10473, and Bugtraq ID 10514.

The memory overflow error on the window() function is reported in a Computer Terrorism article.

More information on the `ADODB.connection` vulnerability is reported in US-CERT Vulnerability Note VU#589272 and Bugtraq ID 20704.

4.7 Java Plugin vulnerability

Impact

An attacker can bypass Java's security restrictions and take unauthorized actions on a victim's computer when the victim visits the attacker's web site.

Resolution

For JDK and JRE, upgrade to version 14.0.2 or higher for 14.x, 11.0.8 or higher for 11.x, 8.0 update 261 or higher, 7.0 update 271 or higher for LTS.

IBM Java, updates can be downloaded at the IBM Java Security alerts page or for IBM Java running stand-alone, information about the available Service Refreshes and Fix Packs can be found at IBM developer kits.

For Oracle JavaFX, the latest release is included with the latest update of JDK and JRE 7 and 8.

Mac OS X updates can be downloaded at the Java Download page.

For the Floating-Point Value Denial of Service vulnerability, patch as designated in the Oracle Security Alert for CVE-2010-4476.

No patch exists for the ActiveX Deployment Toolkit vulnerability. The kill bit for this ActiveX control must be set.

Workaround:
Set the kill bit for the CLSID {CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA} using Microsoft Support: Setting the kill bit.

References

The Oracle Java SE CPU October 2020 was reported in Oracle Critical Patch Update - October 2020.

The Oracle Java SE CPU July 2020 was reported in Oracle Critical Patch Update - July 2020.

The Oracle Java SE CPU April 2020 was reported in Oracle Critical Patch Update - April 2020.

The Oracle Java SE CPU January 2020 was posted to Oracle Critical Patch Update - January 2020.

The Oracle Java SE CPU October 2019 was posted to Oracle Critical Patch Update - October 2019.

For more information on the Oracle Java SE CPU July 2019, see Oracle Critical Patch Update - July 2019.

For more information on the Oracle Java SE CPU April 2019, see Oracle Critical Patch Update - April 2019.

For more information on the Oracle Java SE CPU January 2019, see Oracle Critical Patch Update - January 2019.

For the Oracle Java SE CPU October 2018, see Oracle Critical Patch Update - October 2018.

For the IBM Java file overwrite vulnerability, see swg1IJ08248.

For the IBM Java denial of service vulnerability, see swg1IJ08278.

For the IBM Java "Java Attach API" vulnerability, see swg1IJ08250.

For the IBM Java 8.0 affected by multiple OpenSSL vulnerabilities, see swg1IJ07855.

The vulnerabilities in Oracle JDK and JRE 6.0 update 191 and prior, 7 update 181 and prior, 8 update 171 and prior, and 10.0.1 were posted to Oracle Critical Patch Update - July 2018.

The vulnerabilities in Oracle JDK and JRE 6.0 update 181 and prior, 7 update 171 and prior, 8 update 162 and prior, and 10 and prior were posted to Oracle Critical Patch Update - April 2018.

For the IBM Java Privilege Elevation vulnerability, see swg1IJ04021.

The vulnerabilities in Oracle JDK and JRE 6.0 update 171 and prior, 7 update 161 and prior, 8 update 152 and prior, and 9.0.1 were reported in Oracle Critical Patch Update - January 2018.

The vulnerabilities in Oracle JDK and JRE 6.0 update 161 and prior, 7 update 151 and prior, 8 update 144 and prior were reported in Oracle Critical Patch Update - October 2017.

The vulnerabilities in Oracle JDK and JRE 6.0 update 151 and prior, 7 update 141 and prior, 8 update 131 and prior were reported in Oracle Critical Patch Update - July 2017.

The vulnerabilities in Oracle JDK and JRE 6.0 update 141 and prior, 7 update 131 and prior, 8 update 121 and prior were reported in Oracle Critical Patch Update - April 2017.

The vulnerabilities in Oracle JDK and JRE 6.0 update 131 and prior, 7 update 121 and prior, 8 update 112 and prior were reported in Oracle Critical Patch Update - January 2017.

The vulnerabilities in Oracle JDK and JRE 6.0 update 121 and prior, 7 update 111 and prior, 8 update 102 and prior were reported in Oracle Critical Patch Update - October 2016.

The vulnerabilities in Oracle JDK and JRE 6.0 update 115 and prior, 7 update 101 and prior, 8 update 92 and prior were reported in Oracle Critical Patch Update - July 2016.

The vulnerabilities in Oracle JDK and JRE 6.0 update 113 and prior, 7 update 99 and prior, 8 update 77 and prior were reported in Oracle Critical Patch Update - April 2016.

The vulnerability in Oracle JDK and JRE 7 update 97 and prior, 8 prior to update 77 was reported in CVE-2016-0636.

The vulnerability in Oracle JDK and JRE Executable installers for Windows was reported in CVE-2016-0603.

The vulnerabilities in Oracle JDK and JRE 6.0 update 105 and prior, 7 update 91 and prior, 8 update 66 and prior, and IBM Java were reported in Oracle Critical Patch Update - October 2015.

The IBM Java information disclosure vulnerability was reported in swg21969225.

The vulnerabilities in Oracle JDK and JRE 6.0 update 101 and prior, 7 update 85 and prior, 8 update 60 and prior, IBM Java, and JavaFX were reported in Oracle Critical Patch Update - October 2015.

The vulnerabilities in Oracle JDK and JRE 6.0 update 95 and prior, 7 update 80 and prior, 8 update 45 and prior, JavaFX 2.2.80 were reported in Oracle Critical Patch Update - July 2015.

The vulnerabilities in Oracle JDK and JRE 5.0 update 81 and prior, 6 update 91 and prior, 7 update 76 and prior, 8 update 40 and prior, JavaFX 2.2.76 were reported in Oracle Critical Patch Update - April 2015.

The Two vulnerabilities fixed in IBM Security Update February 2015 were reported in IBM Security Update February 2015.

The vulnerabilities in Oracle JDK and JRE 5.0 update 75 and prior, 6 update 85 and prior, 7 update 72 and prior, 8 update 25 and prior, and IBM Java were reported in Oracle Critical Patch Update - January 2015 and IBM Security Updates Oracle January 20_2015_CPU.

The Secure Transport vulnerability and IBM Java Shared Classes Feature Cache vulnerability were reported in swg21688283.

The vulnerabilities in Oracle JDK and JRE 5.0 update 71, 6 update 81, 7 update 67, 8 update 20, and prior, JavaFX 2.2.65, and IBM Java were reported in Oracle Critical Patch Update - October 2014 and swg21688283.

The vulnerabilities in Oracle JDK and JRE 5.0 update 65, 6 update 75, 7 update 60, 8 update 5, and prior were reported in Oracle Critical Patch Update - July 2014 and IBM Security Updates Oracle_July_15_2014_CPU.

The vulnerabilities in Oracle JDK and JRE 8.0, 7.0 update 51, 6.0 update 71, 5.0 update 61, and JavaFX 2.2.51 were reported in Oracle Critical Patch Update - April 2014.

The vulnerabilities in Oracle JDK and JRE 7.0 update 45, 6.0 update 65, and 5.0 update 55, JavaFX 2.2.45, and prior were reported in Secunia Advisory SA56485, Secunia Advisory SA56594, and Secunia Advisory SA56484.

The vulnerabilities in Oracle JDK and JRE 7.0 update 40, 6.0 update 60, and 5.0 update 51, and JavaFX 2.2.40, and prior were reported in Secunia Advisory SA55315, Secunia Advisory SA55604, and Secunia Advisory SA55316.

The undisclosed vulnerabilities fixed in the July 2013 IBM Security Update were reported in IBM DeveloperWorks.

The vulnerabilities in Oracle JDK and JRE 7.0 update 21, 6.0 update 45, and 5.0 update 45, and JavaFX 2.2.21 and prior were reported in Secunia Advisory SA53846 and Secunia Advisory SA53852.

The vulnerabilities in Oracle JDK and JRE 7.0 update 17, 6.0 update 43, and 5.0 update 41 were reported in Secunia Advisory SA53008.

Multiple Vulnerabilities Fixed in Oracle JavaFX 2.2.21 were reported in Secunia Advisory SA53095 and Oracle Java SE Critical Patch Update Advisory - April 2013.

The vulnerabilities in Oracle JDK and JRE 7.0 update 15, 6.0 update 41, and 5.0 update 40 were reported in Secunia Advisory SA52451.

The vulnerabilities in Oracle JDK and JRE 7.0 update 13, 6.0 update 39, 5.0 update 39, and 1.4.2_41 were reported in Secunia Advisory SA52257.

The vulnerabilities in Oracle JDK and JRE 7.0 update 11, 6.0 update 38, 5.0 update 38, and 1.4.2_40, and JavaFX 2.2.4 and prior were reported in Oracle Java SE Critical Patch Update - February 2013, Secunia Advisory SA52064, and Secunia Advisory SA52065.

The vulnerabilities in Oracle JDK and JRE 7.0 update 10 were reported in Secunia Advisory SA51820, and Oracle Security Alert for CVE-2013-0422.

The vulnerabilities in Oracle JDK and JRE 7.0 update 7, 6.0 update 35, 5.0 update 36, and 1.4.2_38, and JavaFX 2.2 and prior, were reported in Secunia Advisory SA50949.

The multiple vulnerabilities in JDK/JRE 7 Update 6, and 6 Update 34 were reported in Secunia Advisory SA50133, Secunia Advisory SA50498, and Oracle Security Alert for CVE-2012-4681.

The vulnerabilities in Oracle JDK and JRE 7.0 update 4, 6.0 update 32, 5.0 update 35, and 1.4.2_37, and JavaFX 2.1 and prior, were reported in the Oracle Java SE Critical Patch Update - June 2012.

The vulnerabilities in 7.0 update 2, 6.0 update 30, 5.0 update 33, and 1.4.2_35 were reported in Oracle Java SE Critical Patch Update Advisory - February 2012.

The Java Software Update Spoofing vulnerability was reported in Secunia Advisory SA47134.

The multiple vulnerabilities in 7.0, 6.0 update 27, 5.0 update 31, and 1.4.2_33 were reported in Oracle Java SE Critical Patch Update Advisory - October 2011.

The JRE Insecure Executable Loading vulnerability was reported in Secunia Advisory SA45173.

The vulnerabilities in version 6.0 update 25, 5.0 update 29, and 1.4.2_31 were reported in Oracle Java SE Critical Patch Update Advisory - June 2011.

The vulnerabilities in version 6.0 update 23, 5.0 update 27, and 1.4.2_29 were reported in Oracle Java SE and Java for Business Critical Patch Update Advisory - February 2011.

The Floating-Point Value Denial of Service vulnerability was reported in Bugtraq ID 46091.

The vulnerabilities fixed in version 6.0 update 22, 5.0 update 26, 1.4.2_28, and 1.3.1_29 were reported in Oracle Java SE and Java for Business Critical Patch Update Advisory - October 2010.

The `HsbParser.getSoundBank()` Remote Heap Buffer Overflow vulnerability was reported in Bugtraq ID 39559.

The vulnerabilities fixed in version 6.0 update 20 were reported in Oracle Security Alert CVE-2010-0886.

The vulnerabilities fixed in version 6.0 update 19, 5.0 update 24, 1.4.2_26, and 1.3.1_28 were reported in Oracle Java SE and Java for Business Critical Patch Update Advisory - March 2010.

The multiple vulnerabilities fixed in JDK/JRE 6 Update 17 and 5 Update 22, and SDK/JRE 1.4.2_24 and 1.3.1_27 were reported in Bugtraq ID 36881.

The multiple vulnerabilities fixed in JDK/JRE 6 Update 15 and 5 Update 20 were reported in Sun Alert 263408, Sun Alert 263409, Sun Alert 263429, Sun Alert 263488, Sun Alert 263489, and Sun Alert 263490.

The Aqua Look and Feel Privilege Escalation vulnerability was reported in Bugtraq ID 35381.

The deploytk ActiveX buffer overflow vulnerability details can be found in Bugtraq ID 34931.

The multiple vulnerabilities fixed in JDK/JRE 6 Update 13 and 5 Update 18, and SDK/JRE 1.4.2_20 and 1.3.1_25 were reported in Sun Alert 254569, Sun Alert 254570, Sun Alert 254571, Sun Alert 254608, Sun Alert 254609, Sun Alert 254610, and Sun Alert 254611.

The multiple vulnerabilities fixed in JDK/JRE 6 Update 11 and 5 Update 17, and SDK/JRE 1.4.2_19 and 1.3.1_24 were reported in Sun Alert 244986, Sun Alert 244987, Sun Alert 244989, Sun Alert 244990, Sun Alert 244991, Sun Alert 244992, Sun Alert 245246, Sun Alert 246266, Sun Alert 246286, Sun Alert 246346, Sun Alert 246366, Sun Alert 246386, and Sun Alert 246387.

The multiple vulnerabilities fixed in JDK/JRE 6 Update 7 and 5 Update 16, and SDK/JRE 1.4.2_18 and 1.3.1_23 were reported in Sun Alert 238628, Sun Alert 238666, Sun Alert 238687, Sun Alert 238965, Sun Alert 238966, Sun Alert 238967, and Sun Alert 238968.

The multiple vulnerabilities fixed in JDK/JRE 6 Update 5 and 5 Update 15, and SDK/JRE 1.4.2_17 and 1.3.1_22 are described in US Cert Technical Cyber Security Alert TA08-066A and Secunia Advisory SA29239.

The untrusted application/applet privilege elevation vulnerability was reported in Sun Alert 23125.

The XML external entity vulnerability was reported in Sun Alert 231246.

The vulnerabilities fixed in Java for Apple Mac OS X were reported in BugTraq ID 19849, BugTraq ID 22083, BugTraq ID 21675, BugTraq ID 21674, BugTraq ID 21673, BugTraq ID 22085, BugTraq ID 23728, BugTraq ID 24004, BugTraq ID 24690, BugTraq ID 24695, BugTraq ID 24832, BugTraq ID 24846, BugTraq ID 25054, BugTraq ID 25340, BugTraq ID 25918, BugTraq ID 26877, Secunia Advisory SA26402, and Secunia Advisory SA28115.

The vulnerabilities fixed in 6.0 Update 3, 5.0 Update 13, 1.4.2_16 and 1.3.1_21 were reported in Secunia Advisory SA27009.

The JRE Font Processing Overflow was reported in Bugtraq ID 25340.

The JavaDoc cross-site scripting vulnerability was reported in Secunia Advisory SA25769.

The Applet Class Loader vulnerability was reported in BugTraq ID 25054.

The JSSE denial of service vulnerability was reported in BugTraq ID 24846.

The Java XML Digital Signature vulnerability was reported in BugTraq ID 83518.

The JRE image parsing buffer overflow and Java Virtual Machine denial of service were reported in BugTraq ID 24004.

The JDK image processing vulnerabilities were reported in Secunia Advisory SA25295 and CESA-2006-004.

The GIF file handling memory corruption vulnerability was reported in Bugtraq ID 22085.

The abstract windowing toolkit module memory corruption was reported in Bugtraq ID 21675.

The `Font.createFont` Denial of Service was reported in Bugtraq ID 17981.

The reflection API vulnerabilities were reported in BugTraq ID 15615.

The privilege elevation vulnerability for the Java Sandbox was reported in Secunia Advisory SA17748.

The privilege elevation vulnerabilities for the Java Plug-in were reported in BugTraq ID 14238, BugTraq ID 11726, and BugTraq ID 12317.

The second vulnerability was reported in Sun Alert 57708.

For more information on Java security architecture and sandboxes, see the document from Sun.

4.8 last user name disclosure

Impact

An attacker with physical access to the computer could determine a valid user name on the system, thus facilitating password guessing attacks.

Resolution

Run **`regedt32`**, and in the key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`, set `DontDisplayLastUserName` equal to 1.

References

More information is available in The Registry Guide for Windows.

4.9 Mozilla vulnerabilities

Impact

A remote attacker could execute arbitrary commands on a client system, disclose certain sensitive information, crash the system, or bypass certain security restrictions when the client browses to a malicious web site hosted by the attacker.

Resolution

Upgrade to Firefox 83, ESR 78.5 or higher, or 68.12 or higher for Firefox ESR.

Note: The release of 68.12 is the final scheduled for Firefox 68 ESR unless there is a critical security issue found prior to the release of Firefox ESR 78.3 on September 22, 2020. Users of Firefox 68 ESR will be automatically upgraded to the Firefox 78 ESR series with the release of 78.3.

Note: In later versions of Debian, Firefox is known as Iceweasel.

For SeaMonkey, upgrade to 2.38 or higher.

For Cyberfox, upgrade to Cyberfox 41.0.2 or higher.

For Waterfox, upgrade to Waterfox 40.1.0 or higher.

References

For information on most of the above bugs, see Known Vulnerabilities in Mozilla.

For Firefox 78.5 and 83, see mfsa2020-50 and mfsa2020-51.

For Firefox 78.4.1 and 82.0.3, see mfsa2020-49.

For Firefox 82 and ESR 78.4, see mfsa2020-45 and mfsa2020-46.

For Firefox 81 and ESR 78.3, see mfsa2020-42 and mfsa2020-43.

For the ESR 68.12, 78.2, and 80, see mfsa2020-37, mfsa2020-38, and mfsa2020-36.

For the ESR 68.11, 78.1, and 79, see mfsa2020-30, mfsa2020-31, and mfsa2020-32.

For the ESR 68.10 and 78.0, see mfsa2020-24 and mfsa2020-25.

For the ESR 68.9 and 77.0, see mfsa2020-20 and mfsa2020-21.

For the ESR 68.8 and 76.0, see mfsa2020-16 and mfsa2020-17.

For the ESR 68.7 and 75.0, see mfsa2020-12 and mfsa2020-13.

For the ESR 68.6.1 and 74.0.1, see mfsa2020-11.

For the ESR 68.6 and 74, see mfsa2020-09 and mfsa2020-08.

For the ESR 68.5 and 73, see mfsa2020-05 and mfsa2020-06.

For the ESR 68.4.1 and 72.0.1, see mfsa2020-03.

For the ESR 68.4 and 72.0, see mfsa2020-01 and mfsa2020-02.

For the ESR 68.3 and 71.0, see mfsa2019-36 and mfsa2019-37.

For the Mozilla Firefox ESR 68.2 and 70.0 fixed multiple vulnerabilities, see mfsa2019-33 and mfsa2019-34.

For more information regarding Pointer Lock is enabled with no user notification, see mfsa2019-31.

For the Mozilla Firefox ESR 60.9, ESR 68.1 and 69.0 fixed multiple vulnerabilities, see mfsa2019-25, mfsa2019-26, and mfsa2019-27.

For the stored passwords in 'Saved Logins' can be copied without master password entry, see mfsa2019-24.

For the Mozilla Firefox ESR 60.8 and 68.0 fixed multiple vulnerabilities, see mfsa2019-22 and mfsa2019-21.

For the Mozilla Firefox sandbox escape vulnerability using Prompt:Open, see mfsa2019-19.

For the Mozilla Firefox ESR 60.7.1 and 67.0.3 fixed type confusion vulnerability (CVE-2019-11707), see mfsa2019-18.

For the Mozilla Firefox local file access vulnerability (CVE-2019-11702), see mfsa2019-16.

For the Mozilla Firefox ESR 60.7 and 67.0 fixed multiple vulnerabilities, see mfsa2019-13 and mfsa2019-14.

For the Mozilla Firefox 66.0.1 vulnerability fix, see mfsa2019-09 and for Mozilla Firefox ESR 60.6.1 vulnerability fix, see mfsa2019-10.

For the Mozilla Firefox ESR 60.6 and 66.0 fixed multiple vulnerabilities, see mfsa2019-07 and mfsa2019-08.

For the Mozilla Firefox ESR 60.5.1 and 65.0.1 fixed multiple vulnerabilities, see mfsa2019-04 and mfsa2019-05.

For the Mozilla Firefox ESR 60.5 and 65.0 fixed multiple vulnerabilities, see mfsa2019-01 and mfsa2019-02.

For the Mozilla Firefox ESR 60.4 and 64.0 that fixed multiple vulnerabilities, see mfsa2018-29 and mfsa2018-30.

For the Mozilla Firefox ESR 60.3 and 63.0 fixed multiple vulnerabilities, see mfsa2018-26 and mfsa2018-27.

For the Mozilla Firefox ESR 60.2.2 and 62.0.3 fixed two vulnerabilities, see mfsa2018-24.

For the Mozilla Firefox `TransportSecurityInfo` denial of service vulnerability, see mfsa2018-22 and mfsa2018-23.

For the Mozilla Firefox ESR 60.2 and 62 fixed multiple vulnerabilities, see mfsa2018-21 and mfsa2018-20.

For the Mozilla Firefox ESR 52.9, 60.1, and 61.0 fixed multiple vulnerabilities, see mfsa2018-15, mfsa2018-16, and mfsa2018-17.

For the Mozilla Firefox heap buffer overflow in Skia library, see mfsa2018-14.

For the Mozilla Firefox ESR 52.8 and 60.0 fixed multiple vulnerabilities, see mfsa2018-11 and mfsa2018-12.

For the Mozilla use-after-free in compositor, see mfsa2018-10.

For the out of bounds memory write while processing Vorbis audio data, see mfsa2018-08.

For the multiple vulnerabilities fixed in Firefox ESR 52.7 and 59, see mfsa2018-07 and mfsa2018-06.

For the arbitrary code execution through unsanitized browser user interface, see mfsa2018-05.

The multiple vulnerabilities fixed in Firefox ESR 52.6 and 58 were reported in mfsa2018-02 and mfsa2018-03.

The speculative execution side-channel attack was reported in mfsa2018-01.

The buffer overflow fixed in Firefox ESR 52.5.2 and 57.0.2 were reported in mfsa2017-28 and mfsa2017-29.

The two vulnerabilities fixed in Firefox 57.0.1 were reported in mfsa2017-27.

The multiple vulnerabilities fixed in Firefox ESR 52.5 and 57.0 were posted to mfsa2017-24 and mfsa2017-25.

The multiple vulnerabilities fixed in Firefox ESR 52.4 and 56.0 were posted to mfsa2017-21 and mfsa2017-22.

The multiple vulnerabilities fixed in Firefox ESR 52.3 and 55.0 were posted to mfsa2017-19 and mfsa2017-18.

The multiple vulnerabilities fixed in Firefox ESR 52.2 and 54.0 were posted in mfsa2017-15 and mfsa2017-16.

The Mozilla Firefox fixed use-after-free vulnerability in ANGLE was posted in mfsa2017-14.

The multiple vulnerabilities fixed in Firefox 45.9, 52.1, and 53.0 were posted in mfsa2017-11, mfsa2017-12, and mfsa2017-10.

The Mozilla Firefox integer overflow in `createImageBitmap()` was posted in mfsa2017-08.

The multiple vulnerabilities fixed in Firefox 45.8 and 52.0 were posted in mfsa2017-06 and mfsa2017-05.

The multiple vulnerabilities fixed in Firefox 45.7 and 51.0 were posted in mfsa2017-01 and mfsa2017-02.

The multiple vulnerabilities fixed in Firefox 45.6 and 50.1 were reported in mfsa2016-94 and mfsa2016-95.

The Mozilla Firefox SVG Animation Remote Code Execution was reported in mfsa2016-92.

The Mozilla Firefox HTTP Redirect vulnerability fixed in 50.0.1 was reported in mfsa2016-91.

The multiple vulnerabilities fixed in Firefox 45.5 and 50.0 were reported in mfsa2016-89 and mfsa2016-90.

The two vulnerabilities fixed in Firefox 49.0.2 were reported in mfsa2016-87.

The multiple vulnerabilities fixed in Firefox 45.4 and 49.0 were reported in mfsa2016-85 and mfsa2016-86.

The multiple vulnerabilities fixed in Firefox 45.3 and 48.0 were reported in mfsa2016-62 through mfsa2016-84.

The multiple vulnerabilities fixed in Firefox 45.2 and 47.0 were reported in mfsa2016-49 through mfsa2016-61.

The multiple vulnerabilities fixed in Firefox 38.8 and 46.0 were reported in mfsa2016-39 through mfsa2016-48.

The multiple vulnerabilities fixed in Firefox 38.7 and 45.0 were reported in mfsa2016-16 through mfsa2016-38.

The multiple vulnerabilities in LibGraphite Font Processing were reported in mfsa2016-14 and Libgraphite Font Processing Vulnerabilities.

The same-origin-policy violation using Service Workers with plugins was reported in mfsa2016-13.

The multiple vulnerabilities fixed in Firefox 38.6 and 44.0 were reported in mfsa2016-01, mfsa2016-02, mfsa2016-03, mfsa2016-04, mfsa2016-05, mfsa2016-06, mfsa2016-07, mfsa2016-08, mfsa2016-09, mfsa2016-10, mfsa2016-11, and mfsa2016-12.

The MD5 Signatures accepted in TLS ServerKeyExchange was reported in mfsa2015-150 and Bugtraq ID 79684.

The multiple vulnerabilities fixed in Firefox 38.5 and 43.0 were reported in mfsa2015-134, mfsa2015-135, mfsa2015-136, mfsa2015-137, mfsa2015-138, mfsa2015-139, mfsa2015-140, mfsa2015-141, mfsa2015-142, mfsa2015-143, mfsa2015-144, mfsa2015-145, mfsa2015-146, mfsa2015-147, mfsa2015-148, and mfsa2015-149.

The multiple vulnerabilities fixed in Firefox 38.4 and 42.0 were reported in mfsa2015-133, mfsa2015-132, mfsa2015-131, mfsa2015-130, mfsa2015-129, mfsa2015-128, mfsa2015-127, mfsa2015-126, mfsa2015-123, mfsa2015-122, mfsa2015-121, mfsa2015-118, mfsa2015-117, and mfsa2015-116.

The Cross-origin restriction bypass using Fetch was reported in mfsa2015-115.

The multiple vulnerabilities fixed in Firefox 38.3 and 41.0, SeaMonkey 2.38, Cyberfox 41.0, and Waterfox 40.1.0 were reported in mfsa2015-96, mfsa2015-97, mfsa2015-98, mfsa2015-100, mfsa2015-101, mfsa2015-102, mfsa2015-103, mfsa2015-104, mfsa2015-105, mfsa2015-106, mfsa2015-107, mfsa2015-108, mfsa2015-108, mfsa2015-110, mfsa2015-111, mfsa2015-112, mfsa2015-113, mfsa2015-114, and Waterfox 40.1.0.

The two vulnerabilities fixed in Firefox 38.2.1, 40.0.3, and Cyberfox 40.0.3 were reported in mfsa2015-94 and mfsa2015-95.

The libstagefright Vulnerability was reported in mfsa2015-93.

The multiple vulnerabilities fixed in Firefox 38.2, 40.0, and Cyberfox 40.0 were reported in mfsa2015-79, mfsa2015-80, mfsa2015-81, mfsa2015-82, mfsa2015-83, mfsa2015-84, mfsa2015-85, mfsa2015-86, mfsa2015-87, mfsa2015-88, mfsa2015-89, mfsa2015-90, mfsa2015-91, and mfsa2015-92.

The Same origin violation vulnerability was reported in mfsa2015-78.

The multiple vulnerabilities fixed in Firefox 31.8, 38.1, and 39.0 were reported in mfsa2015-59, mfsa2015-60, mfsa2015-61, mfsa2015-62, mfsa2015-63, mfsa2015-64, mfsa2015-65, mfsa2015-66, mfsa2015-67, mfsa2015-68,

mfsa2015-69, mfsa2015-70, and mfsa2015-71.

The multiple vulnerabilities fixed in Firefox 31.7, 38.0, Cyberfox 38.0, and Waterfox 38.0 were reported in mfsa2015-46, mfsa2015-47, mfsa2015-48, mfsa2015-49, mfsa2015-50, mfsa2015-51, mfsa2015-53, mfsa2015-54, mfsa2015-55, mfsa2015-56, mfsa2015-57, mfsa2015-58, and Waterfox 38.0.

The memory corruption during failed plugin initialization was reported in mfsa2015-45.

The SSL certificate verification bypass was reported in mfsa2015-44 and Waterfox 37.0.1 Release.

The multiple vulnerabilities fixed in Firefox 31.6, 37.0, and Cyberfox 37.0 were reported in mfsa2015-30, mfsa2015-31, mfsa2015-32, mfsa2015-33, mfsa2015-34, mfsa2015-35, mfsa2015-36, mfsa2015-37, mfsa2015-38, mfsa2015-39, mfsa2015-40, mfsa2015-41, and mfsa2015-42.

The two vulnerabilities fixed in Firefox 31.5.2 and 36.0.4, SeaMonkey 2.33.1, Cyberfox 36.0.4, and Waterfox 36.0.4 were reported in MFSA 2015-29, MFSA 2015-28, and Waterfox 36.0.4 Release.

The multiple vulnerabilities fixed in Firefox 31.5 and 36, Cyberfox 36.0, and Waterfox 36.0 were reported in Security Advisories for Firefox 36, and Waterfox 36.0 Release.

The multiple vulnerabilities fixed in Firefox 31.4 and 35, SeaMonkey 2.32, Cyberfox 35.0, and Waterfox 35.0 were reported in Security Advisories for Firefox 35, Security Advisories for SeaMonkey 2.32, and Waterfox 35.0 Release.

The Two Vulnerabilities fixed in Firefox 34 and SeaMonkey 2.31 were reported in mfsa2014-91.

The multiple vulnerabilities fixed in Firefox 31.3 and 34, Cyberfox 34.0, and Waterfox 34.0 were reported in Security Advisories for Firefox 34 and Waterfox 34.0 Release.

The multiple vulnerabilities fixed in Firefox 31.2 and, Cyberfox 33.0, and Waterfox 32 were reported in Security Advisories for Firefox 33 and Waterfox 33.0.2 Release.

The RSA signature forgery in NSS was reported in Security Advisories for Firefox 32.0.3.

The multiple vulnerabilities fixed in Firefox 24.8, 31.1, and 32, Cyberfox 32.0.1, and Waterfox 32 were reported in Security Advisories for Firefox 32 and Waterfox 32.0 Release.

The multiple vulnerabilities fixed in Firefox 24.7 and 31, Cyberfox 31, and Waterfox 31 were reported in Security Advisories for Firefox 31 and Waterfox 31.0 Release.

The multiple vulnerabilities fixed in Firefox 24.6 and 30, and Cyberfox 30 were reported in Security Advisories for Firefox 30.

The unspecified vulnerability fixed in Cyberfox 28.0.1 was reported in BugTraq ID 67185.

The multiple vulnerabilities fixed in Firefox 29, SeaMonkey 2.26, and Cyberfox 29.0.1 were reported in Security Advisories for Firefox 29.

The multiple vulnerabilities fixed in Firefox 28, SeaMonkey 2.25 and Cyberfox 28.0 were reported in Secunia Advisory SA57500, Secunia Advisory SA57510, Secunia Advisory SA57505, and Security Advisories for Firefox 28.

The multiple vulnerabilities fixed in Firefox 27, SeaMonkey 2.24, and Cyberfox 27.0 were reported in Secunia Advisory SA56767, Secunia Advisory SA56787, Secunia Advisory SA56706, and Security Advisories for Firefox 27.

The multiple vulnerabilities fixed in Firefox 26, SeaMonkey 2.23, and Cyberfox 26.0 were reported in Secunia Advisory SA56002, Secunia Advisory SA56005, Secunia Advisory SA56050, mfsa2013-104, mfsa2013-105, mfsa2013-106, mfsa2013-107, mfsa2013-108, mfsa2013-109, mfsa2013-111, mfsa2013-112, mfsa2013-113, mfsa2013-114, mfsa2013-115, and mfsa2013-116.

The multiple vulnerabilities fixed in Firefox 25.0.1, SeaMonkey 2.22.1, and Cyberfox 25.0.1 were reported in mfsa2013-103, Secunia Advisory SA55732, and Secunia Advisory SA55766.

The multiple vulnerabilities fixed in Firefox 25.0, SeaMonkey 2.22, and Cyberfox 25.0 were reported in mfsa2013-93, mfsa2013-94, mfsa2013-95, mfsa2013-96, mfsa2013-97, mfsa2013-98, mfsa2013-99, mfsa2013-100, mfsa2013-101, and mfsa2013-102.

The multiple vulnerabilities fixed in Firefox 24.0 and 17.0.9, SeaMonkey 2.21, and Cyberfox 23.0 were reported in mfsa2013-76, mfsa2013-77, mfsa2013-78, mfsa2013-79, mfsa2013-81, mfsa2013-82, mfsa2013-83, mfsa2013-85, mfsa2013-86, mfsa2013-88, mfsa2013-89, mfsa2013-90, mfsa2013-91, mfsa2013-92, and Secunia Advisory SA54821.

The multiple vulnerabilities fixed in Firefox 23.0 and 17.0.8, SeaMonkey 2.20, and Cyberfox 23.0 were reported in mfsa2013-63, mfsa2013-64, mfsa2013-65, mfsa2013-66, mfsa2013-68, mfsa2013-69, mfsa2013-70, mfsa2013-72, mfsa2013-73, mfsa2013-75, and Secunia Advisory SA54385.

The multiple vulnerabilities fixed in Firefox 22.0 and 17.0.7 were reported in mfsa2013-49, mfsa2013-50, mfsa2013-51, mfsa2013-53, mfsa2013-55, mfsa2013-56, and mfsa2013-59.

The multiple vulnerabilities fixed in Firefox 21.0 and 17.0.6 were reported in mfsa2013-41, mfsa2013-42, mfsa2013-44, mfsa2013-45, mfsa2013-46, and mfsa2013-48.

The multiple vulnerabilities fixed in Firefox 20.0 and 17.0.5 and SeaMonkey 2.17 were reported in mfsa2013-30, mfsa2013-31, mfsa2013-32, mfsa2013-34, mfsa2013-35, mfsa2013-36, mfsa2013-37, mfsa2013-38, mfsa2013-39, and mfsa2013-40.

The HTML Editor Use-After-Free vulnerability was reported in mfsa2013-29.

The multiple vulnerabilities fixed in Firefox 19.0 and 17.0.3 and SeaMonkey 2.16 were reported in mfsa2013-21, mfsa2013-22, mfsa2013-23, mfsa2013-24, mfsa2013-25, mfsa2013-26, mfsa2013-27, and mfsa2013-28.

The multiple vulnerabilities fixed in Firefox 17.0.2 and 10.0.12 and SeaMonkey 2.15 were reported in mfsa2013-01, mfsa2013-02, mfsa2013-03, mfsa2013-04, mfsa2013-05, mfsa2013-06, mfsa2013-07, mfsa2013-08, mfsa2013-09, mfsa2013-10, mfsa2013-11, mfsa2013-12, mfsa2013-13, mfsa2013-14, mfsa2013-15, mfsa2013-16, mfsa2013-17, mfsa2013-18, and mfsa2013-19.

The multiple vulnerabilities fixed in Firefox 17.0 and 10.0.11 and SeaMonkey 2.14 were reported in mfsa2012-91, mfsa2012-92, mfsa2012-93, mfsa2012-94, mfsa2012-95, mfsa2012-96, mfsa2012-97, mfsa2012-98, mfsa2012-99, mfsa2012-100, mfsa2012-102, mfsa2012-103, mfsa2012-104, mfsa2012-105, and mfsa2012-106.

The multiple vulnerabilities fixed in Firefox 16.0.2 and 10.0.10 and SeaMonkey 2.13.2 were reported in mfsa2012-90, and Secunia Advisory SA51144.

The multiple vulnerabilities fixed in Firefox 16.0.1 and 10.0.9 and SeaMonkey 2.13.1 were reported in mfsa2012-88, and mfsa2012-89.

The multiple vulnerabilities fixed in Firefox 16 and 10.8 and SeaMonkey 2.13 were reported in mfsa2012-74, mfsa2012-75, mfsa2012-76, mfsa2012-77, mfsa2012-78, mfsa2012-79, mfsa2012-80, mfsa2012-81, mfsa2012-82, mfsa2012-83, mfsa2012-84, mfsa2012-85, mfsa2012-86, and mfsa2012-87.

The multiple vulnerabilities fixed in Mozilla Firefox 15 and SeaMonkey 2.12 were reported in mfsa2012-57, mfsa2012-58, mfsa2012-59, mfsa2012-60, mfsa2012-61, mfsa2012-62, mfsa2012-63, mfsa2012-64, mfsa2012-65, mfsa2012-66, mfsa2012-67, mfsa2012-68, mfsa2012-69, mfsa2012-70, mfsa2012-71, and mfsa2012-72.

The multiple vulnerabilities fixed in SeaMonkey 2.11 were reported in mfsa2012-42, mfsa2012-44, mfsa2012-45, mfsa2012-47, mfsa2012-48, mfsa2012-49, mfsa2012-50, mfsa2012-51, mfsa2012-52, mfsa2012-53, mfsa2012-54, and mfsa2012-56.

The multiple vulnerabilities fixed in Firefox 14.0 and 10.0.6 were reported in mfsa2012-42, mfsa2012-43, mfsa2012-44, mfsa2012-45, mfsa2012-46, mfsa2012-47, mfsa2012-48, mfsa2012-49, mfsa2012-50, mfsa2012-51, mfsa2012-52, mfsa2012-53, mfsa2012-54, mfsa2012-55, and mfsa2012-56.

The multiple vulnerabilities fixed in Firefox 13.0 and 10.0.5 and SeaMonkey 2.10 were reported in mfsa2012-34, mfsa2012-35, mfsa2012-36, mfsa2012-37, mfsa2012-38, mfsa2012-39, and mfsa2012-40.

The multiple vulnerabilities fixed in Firefox 12.0 and 10.0.4 and SeaMonkey 2.9 were reported in mfsa2012-20, mfsa2012-22, mfsa2012-23, mfsa2012-24, mfsa2012-25, mfsa2012-26, mfsa2012-27, mfsa2012-28, mfsa2012-29, mfsa2012-30, mfsa2012-31, mfsa2012-32, and mfsa2012-33.

The multiple vulnerabilities fixed in Firefox 11.0 and 3.6.28 and SeaMonkey 2.8 were reported in mfsa2012-12, mfsa2012-13, mfsa2012-14, mfsa2012-15, mfsa2012-16, mfsa2012-17, mfsa2012-18, and mfsa2012-19.

The `libpng` Integer Overflow vulnerability was reported in Secunia Advisory SA48089.

The `XBL` Binding `Use-After-Free` vulnerability was reported in Secunia Advisory SA48008.

The multiple vulnerabilities fixed in Firefox 10.0 and 3.6.26 and SeaMonkey 2.7 were reported in mfsa2012-01, mfsa2012-03, mfsa2012-04, mfsa2012-05, mfsa2012-06, mfsa2012-07, mfsa2012-08, and mfsa2012-09.

The JAR File Handling vulnerability was reported in Secunia Advisory SA47340.

The multiple vulnerabilities fixed in Firefox 9.0 and SeaMonkey 2.6 were reported in mfsa2011-53, mfsa2011-54, mfsa2011-55, mfsa2011-56, mfsa2011-57, and mfsa2011-58.

The multiple vulnerabilities fixed in Firefox 8.0 and 3.6.24 were reported in mfsa2011-47, mfsa2011-48, mfsa2011-49, mfsa2011-50, mfsa2011-51, and mfsa2011-52.

The multiple vulnerabilities fixed in Firefox 7.0 and 3.6.23 and SeaMonkey 2.4 were reported in mfsa2011-36, mfsa2011-38, mfsa2011-39, mfsa2011-40, mfsa2011-41, mfsa2011-42, mfsa2011-43, mfsa2011-44, and mfsa2011-45.

The multiple vulnerabilities fixed in Mozilla SeaMonkey 2.3 were reported in mfsa2011-33.

The multiple vulnerabilities fixed in Firefox 6.0 and 3.6.20 were reported in mfsa2011-29, and mfsa2011-30.

The multiple vulnerabilities fixed in SeaMonkey 2.2 were reported in Secunia Advisory SA45007.

The multiple vulnerabilities fixed in Firefox 5.0 were reported in Secunia Advisory SA44972.

The multiple vulnerabilities fixed in Firefox 3.6.18 were reported in mfsa2011-19, mfsa2011-20, mfsa2011-21, mfsa2011-22, mfsa2011-23, and mfsa2011-24.

The multiple vulnerabilities fixed in Firefox 3.5.19 and 3.6.17 and 4.0.1 and SeaMonkey 2.0.14 were reported in mfsa2011-12, mfsa2011-13, mfsa2011-14, mfsa2011-15, mfsa2011-16, mfsa2011-17, and mfsa2011-18.

The multiple vulnerabilities fixed in Firefox 3.5.17 and 3.6.14 and SeaMonkey 2.0.12 were reported in mfsa2011-01, mfsa2011-02, mfsa2011-03, mfsa2011-04, mfsa2011-05, mfsa2011-06, mfsa2011-07, mfsa2011-08, mfsa2011-09, and mfsa2011-10.

The Java `LiveConnect` Script Security Bypass vulnerability was reported in Bugtraq ID 45355.

The "`js/src/jsstr.cpp`" UTF-8 Input Validation vulnerability was reported in Bugtraq ID 44919.

The Heap Buffer Overflow Mixing `document.write` and `DOM` Insertion vulnerability was reported in mfsa2010-73.

The multiple vulnerabilities fixed in Firefox 3.5.14 and 3.6.11 and SeaMonkey 2.0.9 were reported in mfsa2010-64,

mfsa2010-65, mfsa2010-66, mfsa2010-67, mfsa2010-68, mfsa2010-69, mfsa2010-70, mfsa2010-71, and mfsa2010-72.

The `Math.random()` Cross Domain Information Disclosure vulnerability was reported in Bugtraq ID 43222.

The multiple vulnerabilities fixed in Firefox 3.5.12 and 3.6.9 and SeaMonkey 2.0.7 were reported in mfsa2010-49, mfsa2010-50, mfsa2010-51, mfsa2010-53, mfsa2010-54, mfsa2010-55, mfsa2010-56, mfsa2010-57, mfsa2010-58, mfsa2010-59, mfsa2010-60, mfsa2010-61, mfsa2010-62, and mfsa2010-63.

The Firefox and SeaMonkey Plugin Parameters Buffer Overflow vulnerability was reported in Bugtraq ID 41842.

The Firefox Plugin Parameter Reference Remote Code Execution vulnerability was reported in Bugtraq ID 41933.

The multiple vulnerabilities fixed in Firefox 3.5.11 and 3.6.7 and SeaMonkey 2.0.6 were reported in mfsa2010-34, mfsa2010-38, mfsa2010-39, mfsa2010-40, mfsa2010-41, mfsa2010-42, mfsa2010-43, mfsa2010-44, mfsa2010-46, and mfsa2010-47.

The multiple vulnerabilities fixed in Firefox 3.5.10 and 3.6.4 and SeaMonkey 2.0.5 were reported in mfsa2010-26, mfsa2010-27, mfsa2010-28, mfsa2010-29, and mfsa2010-30.

The Keyboard Focus Cross Domain Information Disclosure vulnerability was reported in Bugtraq ID 40701.

The Cross Document DOM Node Movement Remote Code Execution vulnerability was reported in mfsa2010-25.

The multiple vulnerabilities fixed in Firefox 3.0.19 and 3.5.9 and 3.6.2 and SeaMonkey 2.0.4 were reported in mfsa2010-16, mfsa2010-17, mfsa2010-18, mfsa2010-19, mfsa2010-20, mfsa2010-21, mfsa2010-23, and mfsa2010-24.

The multiple vulnerabilities fixed in Firefox 3.0.18 and 3.5.8 and 3.6.2 and SeaMonkey 2.0.3 were reported in mfsa2010-09, mfsa2010-10, mfsa2010-11, mfsa2010-12, mfsa2010-13, mfsa2010-14, and mfsa2010-15.

The Firefox `WOFF` Decoder Integer Overflow Remote Code Execution vulnerability was reported in mfsa2010-08.

The multiple vulnerabilities fixed in Firefox 3.0.18 and 3.5.8 and SeaMonkey 2.0.3 were reported in mfsa2010-01, mfsa2010-02, mfsa2010-03, mfsa2010-04, and mfsa2010-05.

The multiple vulnerabilities fixed in Firefox 3.0.16 and 3.5.6 and SeaMonkey 2.0.1 were reported in mfsa2009-65, mfsa2009-66, mfsa2009-67, mfsa2009-68, mfsa2009-69, mfsa2009-70, and mfsa2009-71.

The Mozilla Firefox `libpr0n GIF` File Handling Denial of Service was reported in Bugtraq ID 37107.

The multiple vulnerabilities fixed in Firefox 3.0.15 and 3.5.4 and SeaMonkey 2.0 were reported in mfsa2009-52, mfsa2009-54, mfsa2009-55, mfsa2009-56, mfsa2009-57, mfsa2009-59, mfsa2009-61, mfsa2009-62, mfsa2009-63, and mfsa2009-64.

The multiple vulnerabilities fixed in Firefox 3.0.14 were reported in mfsa2009-47, mfsa2009-48, mfsa2009-49, mfsa2009-50, and mfsa2009-51.

The Mozilla Firefox and Seamonkey Regular Expression Parsing Heap Buffer Overflow was reported in Bugtraq ID 35891.

The multiple vulnerabilities fixed in Firefox 3.5.2 were reported in mfsa2009-38, mfsa2009-44, mfsa2009-45, and mfsa2009-46.

The multiple vulnerabilities fixed in Firefox 3.0.12 were reported in mfsa2009-34, mfsa2009-35, mfsa2009-36, mfsa2009-37, mfsa2009-39, and mfsa2009-40.

The Multipart Alternative Message Memory Corruption vulnerability was reported in Bugtraq ID 35461.

The `JIT` escape Function Memory Corruption vulnerability was reported in Bugtraq ID 35660.

The `nsViewManager.cpp` Denial of Service vulnerability was reported in Bugtraq ID 35413.

The Web Proxy Redirect Handling Man In The Middle vulnerability was reported in Bugtraq ID 35412.

The multiple vulnerabilities fixed in Firefox 3.0.11 and SeaMonkey 1.1.17 were reported in mfsa2009-24, mfsa2009-25, mfsa2009-26, mfsa2009-27, mfsa2009-28, mfsa2009-29, mfsa2009-30, mfsa2009-31, and mfsa2009-32.

The multiple vulnerabilities fixed in Firefox 3.0.9 and SeaMonkey 1.1.17 were reported in mfsa2009-14, mfsa2009-15, mfsa2009-16, mfsa2009-17, mfsa2009-18, mfsa2009-19, mfsa2009-20, mfsa2009-21, and mfsa2009-22.

The Firefox XUL parser denial of service was reported in Mozilla bug 485941.

The Firefox `ClearTextRun` Function Memory Corruption vulnerability was reported in mfsa2009-23.

The Firefox `_moveToEdgeShift` Remote Code Execution vulnerability was reported in mfsa2009-13.

The `XSL` Transformation Memory Corruption vulnerability was reported in mfsa2009-12.

The multiple vulnerabilities fixed in Firefox 3.0.7 and SeaMonkey 1.1.15 were reported in mfsa2009-07, mfsa2009-08, mfsa2009-09, and mfsa2009-11.

The multiple vulnerabilities fixed in Firefox 3.0.6 and SeaMonkey 1.1.15 were reported in mfsa2009-01, mfsa2009-02, mfsa2009-03, mfsa2009-04, mfsa2009-05, and mfsa2009-06.

The multiple vulnerabilities fixed in Firefox 2.0.0.19 and 3.0.5 and SeaMonkey 1.1.14 were reported in mfsa2008-59, mfsa2008-60, mfsa2008-61, mfsa2008-62, mfsa2008-63, mfsa2008-64, mfsa2008-65, mfsa2008-66, mfsa2008-67, mfsa2008-68, and mfsa2008-69.

The multiple vulnerabilities fixed in Firefox 2.0.0.18 and 3.0.4 and SeaMonkey 1.1.13 were reported in mfsa2008-48, mfsa2008-49, mfsa2008-50, mfsa2008-51, mfsa2008-52, mfsa2008-53, mfsa2008-54, mfsa2008-55, mfsa2008-56, mfsa2008-57, and mfsa2008-58.

The User Interface Event Dispatcher vulnerability was posted to Bugtraq ID 31476.

The SeaMonkey Newsgroup Cancel Message Handling Buffer Overflow was reported in Bugtraq ID 31411.

The multiple vulnerabilities fixed in Firefox 2.0.0.17 and 3.0.2 and SeaMonkey 1.1.12 were reported in mfsa2008-37, mfsa2008-38, mfsa2008-39, mfsa2008-40, mfsa2008-41, mfsa2008-42, mfsa2008-43, mfsa2008-44, and mfsa2008-45.

The vulnerabilities fixed in Firefox 3.0.1 and 2.0.0.16 were reported in mfsa2008-35, and mfsa2008-36.

The CSS Objects Handling Code Execution vulnerability was reported in Secunia Advisory SA30761.

The vulnerabilities in Firefox 2.0.0.9 were reported in Secunia Advisory SA27605, BugTraq ID 85250, and BugTraq ID 26385.

The TLS Client user activities tracking and improper file type handling vulnerabilities were reported in Bugtraq ID 25543 and Bugzilla 395399.

The status bar spoofing vulnerability in Firefox 2.0.0.7 was reported in Bugtraq archive 475467.

The `wyciwyg` vulnerability was reported in Bugtraq ID 24831.

The field focus security bypass was reported in Secunia Advisory SA25904.

The Internet Explorer firefoxurl:// URI vulnerability was reported in Secunia Advisory SA25984.

The file type extension bypass was reported in Bugtraq ID 24447.

The vulnerabilities in 2.0.0.4 were reported in Larholm: unpatched-input-validation-flaw-in-firefox-2004, Bugtraq ID 24286, and Bugtraq ID 24293.

The HREF tag denial of service vulnerability was reported in Bugtraq ID 23747.

The CRLF injection vulnerability in 2.0.0.3 was reported in Bugtraq ID 23668.

The vulnerabilities in Firefox 2.0.0.2 and SeaMonkey 1.0.8 were reported in Bugtraq ID 22601 and Bugtraq ID 22666.

The vulnerabilities in 2.0.0.1 were reported in Secunia Advisory SA24175, Bugtraq archive 459265, Mozilla bug tracking 356355, and Bugtraq archive 454058.

The vulnerabilities in 1.5.0.9 were reported in Bugtraq archive 459162.

The user credential vulnerability was reported in Secunia Advisory SA23046.

The FTP denial of service was reported in Bugtraq ID 19678.

The Linux specific vulnerabilities corrected in Firefox 1.5.0.7 and SeaMonkey 1.0.5 were reported in Secunia Advisory SA21270.

See Secunia Advisory SA16764 for more information on the IDN buffer overflow.

See Bugtraq for more information on the image dragging, security manager bypass, and flash vulnerabilities.

The **`news://`** URL handling flaw was posted to Bugtraq archive 385709.

The download dialog box and local image file access vulnerabilities in Firefox were reported in Secunia Advisory SA13144.

The vulnerabilities in Mozilla 1.7.2 and Firefox 0.9.3 were reported in US-CERT Alert TA04-261A.

The **`SOAPParameter`** integer overflow was reported in iDEFENSE advisory 08.02.04.

The shell request processing vulnerability was reported by Mozilla and in US-CERT Vulnerability Note VU#927014.

The Firefox certificate spoofing problem was posted to Bugtraq archive 369953.

The frame injection vulnerability was reported in Secunia Advisory SA11978.

4.10 SMB protocol version

Impact

Legacy SMB protocols could expose various vulnerabilities or allow man-in-the-middle attacks.

Resolution

Disable SMB1 as instructed in Microsoft Knowledge Base article 2696547. (Note: this will adversely affect compatibility with Windows Server 2003 and older.)

References

For more information about the drawbacks of SMB1, see Stop Using SMB1.

4.11 SMB Signing

Impact

Attackers could perform a man-in-the-middle attack to tamper with communications between Windows machines.

Resolution

Configure the computer to require SMB Signing as follows:

1. Open the *Local Security Policy* (commonly found under *Administrative Tools*)
2. In the left pane, expand *Local Policies*
3. Click on *Security Options*
4. In the right pane, double-click on *Microsoft network server: Digitally sign communications (always)*
5. Choose *Enabled*
6. Click on *OK*

Note: The above steps may affect compatibility with older systems.

References

For more information about SMB Signing, see The Basics of SMB Signing in the Microsoft blogs.

4.12 SSL short block size

Impact

A remote attacker with the ability to sniff network traffic could decrypt long-lived sessions.

Resolution

Disable ciphers which have a 64-bit block size, such as Triple-DES as follows:

- **Apache/OpenSSL:** Upgrade to OpenSSL 1.1.0, which disables Triple-DES ciphers by default. Alternatively, upgrade to OpenSSL 1.0.1u or 1.0.2i or higher, which classify Triple-DES ciphers as MEDIUM, and insert **`!MEDIUM`** in the **`SSLCipherSuite`** directive in the appropriate web server configuration file.
- **IIS:** Disable **`DES`** and **`3DES`** ciphers as described in Microsoft Knowledge Base Article 245030.
- **OpenSSH:** Add or modify the **`Ciphers`** setting in the **`sshd_config`** file and set it to **`aes128-ctr,aes192-ctr,aes256-ctr`**.
- **Windows ISAKMP:** From the Control Panel, go to *Administrative Tools*, then *Local Security Policy*. Click on *IP Security Policies on Local Computer*. Double-click on the active security policy to open its properties. Go to the *General* tab, and click on the *Settings* button, then the *Methods* button. Highlight any security methods whose encryption type is DES or 3DES, and either remove them, or edit them and change the encryption type.
- **Cisco ISAKMP:** Enter the command **`crypto isakmp policy encryption aes-256`**. For more information see Configuring IPsec and ISAKMP.
- Other: See the documentation for the software or device for information on disabling Triple-DES.

Note: disabling Triple-DES ciphers may affect compatibility with older clients.

References

For more information on the SWEET32 attack, see sweet32.info and the BugTraq ID 92630.

4.13 TCP timestamps

Impact

A remote attacker could possibly determine the amount of time since the computer was last booted.

Resolution

TCP timestamps are generally only useful for testing, and support for them should be disabled if not needed.

To disable TCP timestamps on Linux, add the following line to the **`/etc/sysctl.conf`** file:

```
net.ipv4.tcp_timestamps = 0
```

To disable TCP timestamps on Windows, set the following registry value:

Key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters`
Value: `Tcp1323Opts`
Data: 0 or 1

To disable TCP timestamps on Cisco, use the following command:

```
no ip tcp timestamp
```

References

More information on TCP timestamps and round-trip time measurement is available in RFC1323 and Microsoft Article 224829.

4.14 TLS and SSL Protocols

Impact

The use of outdated TLS and SSL protocols could allow various man-in-the-middle attacks.

Resolution

Only TLS 1.1 and 1.2 are considered secure. All older versions of the TLS and SSL protocols should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file. (The -TLSv1 argument requires Apache 2.2.24 or higher or an update from your Linux vendor.)

  ```
  SSLProtocol all -SSLv2 -SSLv3 -TLSv1
  ```

- **IIS:** See KB245030 and KB187498.
- **Other:** Consult the web server documentation.

References

The PCI Security Standards Council published a document titled Migrating from SSL and Early TLS which explains the risks of using SSL and TLS 1.0.

4.15 Web server default page

Impact

An unconfigured web server creates an unnecessary security exposure on the network.

Resolution

Disable unconfigured web servers. If the web server is needed, replace the default page with some appropriate site-specific content.

References

For more information about default web pages, see about.com.

4.16 Windows account policy

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

References

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

4.17 Windows default account names

Impact

The default administrator and guest account names give attackers a starting point for conducting brute-force password guessing attacks.

Resolution

Change the name of the administrator and guest accounts. To do this on Active Directory servers, open *Active Directory Users and Computers*. Click *Users*, then right-click on Administrator or Guest, and select *Rename*. To do this on workstations, open the *Local Security Policy* from the Administrative Tools menu. Choose *Local Policies*, then *Security Options*, then Accounts: Rename administrator or guest account.

References

For more information on securing the administrator account, see The Administrator Accounts Security Planning Guide - Chapter 3.

4.18 Windows password expiration

Impact

If a password becomes compromised, it can be used to gain unauthorized access for an unlimited period of time.

Resolution

Enable password expiration for all users. This is done by removing the check mark beside *password never expires* in the user's properties.

References

More information on best practices related to password security is available from Microsoft.

4.19 Windows PowerShellGet vulnerabilities

Impact

Vulnerabilities in Windows PowerShellGet allow a security policy bypass, leading to arbitrary code execution.

Resolution

Upgrade to PowerShellGet 2.2.5 or higher.

References

For more information on the WDAC security feature bypass, refer to Microsoft advisory CVE-2020-16886.

4.20 Windows updates needed

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

References

For more information on critical updates, see the Windows critical update pages which are available for Windows XP, Windows Vista, Windows Server 2003, Windows 7, Windows Server 2008 and Windows Server 2008 R2, Windows 8.1, Windows 10, and Windows Server 2012 and Windows Server 2012 R2.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Microsoft Lync Server 2013 elevation of privilege vulnerability fixed in July	The July 2020 security update for Microsoft Lync Server 2013 addressed	Security Guidance	

2020 security update	an elevation of privilege vulnerability. (CVE 2020-1025)		
Microsoft Windows Defender elevation of privilege vulnerability	The July 2020 security update for Microsoft Windows Defender addressed an elevation of privilege vulnerability. (CVE 2020-1461)	CVE-2020-1461	
Microsoft Windows Defender MpCmdRun.exe vulnerabilities	The June 2020 update for Microsoft Windows Defender fixed two elevation of privilege vulnerabilities. These vulnerabilities exist due to improper handling of file operations. (CVE 2020-1163, CVE 2020-1170)	Security Guidance	
Microsoft Skype for Business 2015 - Lync 2013 information disclosure	The July 2019 update for Skype for Business 2015 - Lync 2013 fixed an information disclosure vulnerability. The vulnerability exists due to improper handling of display names when they contain non-printable characters. (CVE 2019-1084)	Security Guidance	
Data Sharing Service Elevation of Privilege	An elevation of privilege vulnerability in `dssvc.dll`, a local service that provides data brokering between applications. (CVE)		Bugtraq ID 105726
SharePoint Foundation 2010 Elevation of Privilege	Fixes problems which could allow elevation of privilege if a user opens a specially crafted Office file. (CVE 2018-8155)	Security Guidance	
SharePoint Server 2013 Remote Code Execution	Fixes a problem in which could allow remote code execution if a user opens a specially crafted Office file. (CVE 2017-8742)	Security Guidance	
Windows NT 4.0 Post SP-6a Security Rollup Pack	Bundle of security hotfixes released since Windows NT 4.0 Service Pack 6a.	**NT:** Q299444	
Windows 2000 Post SP 2 Security Rollup Pack	Bundle of security hotfixes released since Windows 2000 Service Pack 2.	**2000:** Q311401 or SP3 or SP4	
Relative Shell Path	Fixes a problem in which an attacker could cause an alternate **`Explorer.exe`** program to run when another user logs in, resulting in arbitrary code execution. (CVE 2000-0663)	**NT:** Q269049 or Q299444 **2000:** Q269049 or SP2 or SP3 or SP4 **XP:** Not Affected	00-052
RPC Denial of Service	Fixes vulnerabilities in various Windows RPC services which could allow an attacker to cause a denial of service. (CVE 2001-0509)	**NT:** Q299444 **2000:** Q298012 or Q311401 or SP3 or SP4 **XP:** Not Affected	01-041
Unchecked Buffer in UPnP Hotfix	Fixes two vulnerabilities: (1) a buffer overflow which would allow an attacker to take complete control over the computer; and (2) a denial-of-service vulnerability. (CVE 2001-0876, CVE 2001-0877)	**NT:** Not Affected **2000:** Not Affected **XP:** Q315000 or SP1 or SP2	01-059
Java Applet Redirect Hotfix	Fixes two vulnerabilities in Microsoft Virtual Machine. (CVE 2002-0058 CVE 2002-0076)	**NT:** Q300845 or 810030 **2000:** Q300845 or 810030 or SP3 or SP4	02-013

		XP: Q300845 or 810030 or SP1 or SP2	
Windows Shell Unchecked Buffer Hotfix	Fixes a buffer overflow condition in the Windows shell that could allow a local attacker to execute arbitrary code at the user's privilege level. (CVE 2002-0070)	**NT:** Q313829 **2000:** Q313829 or SP3 or SP4 **XP:** Not Affected	02-014
Multiple UNC Provider Hotfix	Fixes a vulnerability in Windows' Multiple Uniform Naming Convention Provider which could allow an attacker to gain Local System privileges. (CVE 2002-0151)	**NT:** Q311967 **2000:** Q311967 or SP3 or SP4 **XP:** Q311967 (32 bit) or Q311967 (32 bit embedded) or Q311967 (64 bit) or SP1 or SP2	02-017
Windows debugger authentication Hotfix	Fixes an authentication flaw in the Windows debugger which could allow a local user to execute commands with the privileges of the operating system. (CVE 2002-0367)	**NT:** Q320206 **2000:** Q320206 or SP3 or SP4 **XP:** Not Affected	02-024
Remote Access Service Phonebook Hotfix	Eliminates an unchecked buffer vulnerability which could allow an unprivileged user to gain complete control over the machine hosting the RAS Phonebook. (CVE 2002-0366)	**NT:** Q318138 **2000:** Q318138 or SP3 or SP4 **XP:** Q318138 or SP1 or SP2	02-029
Network Connection Manager Hotfix	Fixes a vulnerability in the Network Connection Manager which could allow a local attacker to gain Local System privileges. (CVE 2002-0720)	**NT:** Not Affected **2000:** Q326886 or SP4 **XP:** Not Affected	02-042
Unchecked Buffer in Network Share Provider Hotfix	Eliminates an unchecked buffer associated with the Server Message Block (SMB) protocol that could lead to Denial of Service (DoS). (CVE 2002-0724)	**NT:** Q326830 **2000:** Q326830 or SP4 **XP:** Q326830 or SP1 or SP2	02-045
Certificate Validation Flaw Hotfix	Eliminates a security vulnerability (associated with the validation of digital certificate chains) that could permit identity spoofing. (CVE 2002-0862)	**NT:** Q329115 **2000:** Q329115 or SP4 **XP:** Q329115 or SP2	02-050
VM JDBC Classes Hotfix	Eliminates three vulnerabilities in Microsoft Virtual Machine's Java Database Connectivity classes which could allow code execution from a malicious web site or e-mail message. (CVE 2002-0865 CVE 2002-0866 CVE 2002-0867)	**NT:** Q329077 or 810030 **2000:** Q329077 or 810030 or SP4 **XP:** Q329077 or 810030 or SP2	02-052
Help Facility Hotfix	Fixes two vulnerabilities in the Windows Help Facility, one in the ActiveX Control (CVE 2002-0693) and another in the processing of **.chm** files (CVE 2002-0694), which could allow code execution from a remote web site or mail message.	**NT:** Q323255 **2000:** Q323255 **XP:** Q323255 (32-bit) or Q323255 (32-bit Embedded w/ SP1 or Q323255 (64-bit) or SP2	02-055
Microsoft Internet Messaging API (MS16-126)	MS16-126 resolves an information disclosure vulnerability in Microsoft Windows in the Microsoft Internet	**Vista** KB3193515, KB3193515 (64 bit),	16-126

	Messaging API. A successful attack would reveal if a file exists on the target machine. (CVE 2016-3298)	**2008:** KB3193515, KB3193515 (64 bit), **7:** KB3192391, KB3192391 (64 bit), **2008 R2:** KB3192391	
VM COM object access Hotfix	Fixes eight vulnerabilities in Microsoft Virtual Machine, including a vulnerability which could allow a Java applet to access COM objects. (CVE 2002-1257 CVE 2002-1258 CVE 2002-1260 CVE 2002-1262 CVE 2002-1286 CVE 2002-1292 CVE 2002-1295)	**NT:** 810030 **2000:** 810030 or SP4 **XP:** 810030 or SP2	02-069
Windows XP shell buffer overflow Hotfix	Fixes a buffer overflow in the Windows XP shell which could allow an attacker to run commands via a **.MP3** or **.WMA** file with corrupt custom attributes. (CVE 2002-1327)	**NT:** not affected **2000:** not affected **XP:** 32-bit: Q329390 or SP2 64-bit: Q329390 or SP2	02-072 CA-2002-37
VM ByteCode Verifier Hotfix	Fixes the ByteCode Verifier to check for illegal commands when loading Java applets, thus preventing attacks from remote web pages and e-mail messages. (CVE 2003-0111)	**NT:** 816093 **2000:** 816093 or SP4 **XP:** 816093 or SP2	03-011
Kernel Debugger Hotfix	Fixes a flaw in the way the kernel passes error messages to the debugger which could allow a local attacker to gain system privileges. (CVE 2003-0112)	**NT:** 811493 **2000:** 811493 or SP4 **XP:** 32-bit: 811493 or SP2 64-bit: 811493 or SP2	03-013
Windows Media Player skins filename decoding Hotfix	Fixes a problem which could allow a web site or e-mail message to save **.wmz** files to arbitrary directories, leading to command execution. (CVE 2003-0228)	**Media Player 7.1:** 817787 **Media Player 8.0:** 817787	03-017
ntdll.dll Hotfix	Fixes a buffer overflow in a core operating system component which can be exploited through many possible attack vectors, including IIS with WebDAV. (CVE 2003-0109)	**NT:** 815021 **2000:** 815021 or SP4 **XP:** 32-bit: 815021 or SP2 64-bit: 815021 or SP2	03-007
NetMeeting directory traversal fix	Fixes a directory traversal vulnerability allowing an attacker to write files anywhere on the disk, leading to code execution. (CVE 2003-0505 CVE 2003-0506)	**NT:** not affected **2000:** SP4 **XP:** SP1 or SP2 **2003:** not affected	Bugtraq ID 7931
ShellExecute API fix	Fixes a buffer overflow in the ShellExecute API function which could be exploitable through any application which uses the function. (CVE 2003-0503)	**NT:** not affected **2000:** SP4 **XP:** not affected **2003:** not affected	SNS-65
HTML Converter fix	Fixes a buffer overflow in the HTML file conversion feature which could allow	**NT:** 823559 **2000:** 823559 or	03-023 CA-2003-14

	an attacker to run commands via a malicious web page or HTML e-mail message. (CVE 2003-0469)	SP4 Update Rollup 1 **XP:** 32-bit: 823559 or SP2 64-bit: 823559 or SP2 **2003:** 32-bit: 823559 or SP1 64-bit: 823559 or SP1	
RPC buffer overflow fix	Fixes a buffer overflow in the DCOM interface to RPC which could allow a remote attacker to execute arbitrary commands. (CVE 2003-0352)	**NT:** 823980 **2000:** 823980 or SP4 Update Rollup 1 **XP:** 32-bit: 823980 or SP2 64-bit: 823980 or SP2 **2003:** 32-bit: 823980 or SP1 64-bit: 823980 or SP1	03-026 CA-2003-16
DirectX buffer overflow fix	Fixes a vulnerability in the Windows DirectX component which could allow an attacker to run commands via a malformed MIDI file. *Note:* If you have installed DirectX 9.0b or higher you are not vulnerable. (CVE 2003-0346)	**NT:** 819696 **2000:** 819696 or SP4 Update Rollup 1 or DirectX 9.0b or later **XP:** 32-bit: 819696 or SP2 or DirectX 9.0b or later 64-bit: 819696 or SP2 or DirectX 9.0b or later **2003:** 32-bit: 819696 or DirectX 9.0b or later or SP1 64-bit: 819696 or DirectX 9.0b or later or SP1	03-030 CA-2003-18
ActiveX Controls	Even if a vulnerable control is locally patched or removed, a website can still instruct a client to download and install the vulnerable control and then exploit the hole. Example: **`mciwndx.ocx`**.	Set the kill bit for the vulnerable CLSID to keep IE from downloading the vulnerable control again.	BugTraq ID 8413
RPCSS Buffer Overflow	Fixes multiple buffer overflow vulnerabilities in the RPCSS DCOM activation code that could enable an attacker to run arbitrary code on a user's system. (CVE 2003-0715 CVE 2003-0528 CVE 2003-0605)	**NT:** Workstation: 824146 **NT:** Server: 824146 **2000:** 824146 or SP4 Update Rollup 1 **XP:** 32-bit: 824146 or SP2 64-bit: 824146 or SP2 64-bit Version	03-039 CA-2003-23

		2003: 824146 or SP2 **2003:** 32-bit: 824146 or SP1 64-bit: 824146 or SP1	
Windows Media Player URL script execution	Adds protection against execution of unauthorized scripts embedded in audio or video streams. (CVE 2003-1107)	**NT:** 828026 **2000:** 828026 **XP:** 828026 or SP2 **2003:** 828026	828026
Authenticode verification vulnerability	Fixes a vulnerability which could allow an attacker to install and run an untrusted ActiveX control, either via a malicious web page or an HTML e-mail. (CVE 2003-0660)	**NT:** 823182 **2000:** 823182 or SP4 Update Rollup 1 **XP:** 823182 or SP2 **2003:** 823182 or SP1	03-041 CA-2003-27
NetBIOS Name Service information disclosure	Fixes an Information Disclosure vulnerability which could allow an attacker to receive random data from the target system's memory. (CVE 2003-0661)	**NT:** 824105 **2000:** 824105 **XP:** 824105 **2003:** 824105	03-034
Troubleshooter ActiveX control vulnerability	Fixes a vulnerability in the Windows troubleshooter application which could allow an attacker to execute commands via a malicious web page or HTML e-mail. (CVE 2003-0662)	**NT:** 826232 **2000:** 826232 or SP4 Update Rollup 1 **XP:** 826232 or SP2 **2003:** 826232 or SP1	03-042 CA-2003-27
Windows messenger service buffer overflow	Fixes a vulnerability which could allow a remote attacker to execute arbitrary commands with Local System privileges. (CVE 2003-0717)	**NT:** 828035 **2000:** 828035 or SP4 Update Rollup 1 **XP:** 828035 or SP2 **2003:** 828035 or SP1	03-043 CA-2003-27
Workstation Service Elevation of Privilege	Fixes an overflow vulnerability which could allow remote command execution when the client receives a specially crafted RPC message. (CVE 2009-1544)	971657	09-041
Windows workstation service buffer overflow	Fixes a vulnerability which could allow a remote attacker to execute arbitrary commands with Local System privileges. (CVE 2003-0812)	**NT:** not affected **2000:** 828749 or SP4 Update Rollup 1 **XP:** 32-bit/64-bit: 828749 or SP2 64-Bit Version 2003: not affected **2003:** not affected	03-049 CA-2003-28
Windows Help and Support Center buffer overflow	Fixes a vulnerability in the code which handles the HCP protocol which could allow an attacker to execute commands with System privileges via	**NT:** 825119 **2000:** 825119 or SP4 Update Rollup 1	03-044 CA-2003-27

	a malicious web page. (CVE 2003-0711)	**XP:** 825119 or SP2 **2003:** 825119 or SP1	
Windows ListBox and ComboBox buffer overflow	Fixes a vulnerability in Windows controls which could allow a local user to gain elevated privileges. (CVE 2003-0659)	**NT:** 824141 **2000:** 824141 or SP4 Update Rollup 1 **XP:** 824141 or SP2 **2003:** 824141 or SP1	03-045 CA-2003-27
Microsoft Data Access Components patch needed	Fixes a vulnerability in MDAC which could allow remote code execution. (CVE 2003-0353 CVE 2003-0903)	**NT/2000:** 832483 **XP:** 832483 or SP2 **2003:** 832483 or SP1	04-003
ASN.1 buffer overflow	Fixes a vulnerability in ASN.1 which could allow remote code execution. (CVE 2003-0818)	**NT:** 828028 **2000:** 828028 or SP4 Update Rollup 1 **XP:** 828028 or SP2 **2003:** 828028 or SP1	04-007
Multiple vulnerabilities (MS04-011)	Fixes 14 vulnerabilities announced in Microsoft bulletin MS04-011, the most critical of which could allow remote code execution. (CVE 2003-0533 CVE 2003-0663 CVE 2003-0719 CVE 2003-0806 CVE 2003-0906 CVE 2003-0907 CVE 2003-0908 CVE 2003-0909 CVE 2003-0910 CVE 2004-0117 CVE 2004-0118 CVE 2004-0119 CVE 2004-0120 CVE 2004-0123)	**NT:** 835732 **2000:** 835732 or SP4 Update Rollup 1 **XP:** 835732 or SP2 **2003:** 835732 or SP1	04-011 TA04-104A
RPC runtime library vulnerability	Fixes a race condition which could allow an attacker to take control of a system, and fixes three other RPC vulnerabilities. (CVE 2003-0807 CVE 2003-0813 CVE 2004-0116 CVE 2004-0124)	**NT:** 828741 **2000:** 828741 or SP4 Update Rollup 1 **XP:** 828741 or SP2 **2003:** 828741 or SP1	04-012 TA04-104A
Jet Database Engine buffer overflow	Fixes a vulnerability which could allow an attacker to take control of a computer by sending a specially crafted database query to an application using Jet. (CVE 2004-0197)	**NT:** 837001 **2000:** 837001 or SP4 Update Rollup 1 **XP:** 837001 or SP2 **2003:** 837001 or SP1	04-014 TA04-104A
HCP URL validation vulnerability	Fixes a vulnerability in the Help and Support Center which could allow an attacker to control a computer via a malicious web page or HTML e-mail message. (CVE 2004-0199)	**NT/2000:** not affected **XP:** 840374 or SP2 **2003:** 840374 or SP1	04-015

Task Scheduler buffer overflow	Fixes a vulnerability which could allow an attacker to execute commands via a malicious web page or a specially crafted **.job** file. (CVE 2004-0212)	**NT:** (with IE6) 841873 **NT:** (without IE6) not affected **2000:** 841873 or SP4 Update Rollup 1 **XP:** 841873 or SP2 **XP:** (64-bit) 841873 or SP2	04-022
HTML Help and showHelp vulnerability	Fixes vulnerabilities in HTML Help and showHelp which could allow code execution via a malicious web page or e-mail message. (CVE 2003-1041 CVE 2004-0201)	**NT:** 840315 **2000:** 840315 or SP4 Update Rollup 1 **XP:** 840315 or SP2 **2003:** 840315 or SP1	04-023
Windows Shell API CLSID vulnerability	Fixes a vulnerability which could allow an attacker to send a class identifier which could persuade a user to run malicious code. (CVE 2004-0420)	**NT:** 839645 **2000:** 839645 or SP4 Update Rollup 1 **XP:** 839645 or SP2 **2003:** 839645 or SP1	04-024
Utility Manager privilege elevation	Fixes a vulnerability which could allow any logged-on user to force Utility Manager to start an application with system privileges. (CVE 2004-0213)	**NT:** not affected **2000:** 842526 or SP4 Update Rollup 1 **XP:** not affected **2003:** not affected	04-019
POSIX subsystem buffer overflow	Fixes a buffer overflow which could allow a locally logged-on user to take full control of the computer. (CVE 2004-0210)	**NT:** 841872 **NT:** (server) 841872 **2000:** 841872 or SP4 Update Rollup 1 **XP:** not affected **2003:** not affected	04-020
GDI+ component JPEG buffer overflow	Fixes a buffer overflow in the Graphics Device Interface which could allow code execution when an application opens a malformed image. (CVE 2004-0200)	**XP:** 833987 **2003:** 833987 or SP1 **Other:** See list of affected products in MS04-028	04-028 TA04-260A
application start vulnerability in Windows shell	Fixes a buffer overflow which could allow an attacker to execute commands when the shell starts an application. (CVE 2004-0214 CVE 2004-0572)	841356	04-037
Compressed folder buffer overflow	Fixes a buffer overflow in the processing of compressed files which could allow code execution via a malicious web page or e-mail message. (CVE 2004-0575)	**NT:** not affected **2000:** not affected **XP:** 873376 (64-bit): 873376 **2003:** 873376 or SP1	04-034

		(64-bit): 873376 or SP1	
Metafile rendering buffer overflow	Fixes four vulnerabilities, the most critical of which could allow code execution via a malformed WMF or EMF image. (CVE 2004-0207 CVE 2004-0208 CVE 2004-0209 CVE 2004-0211)	840987	04-032
Windows NT RPC runtime library denial of service	Fixes a buffer overflow which allows a remote attacker to crash the system or read portions of active memory. (CVE 2004-0569)	**NT:** 873350 **2000:** not affected **XP:** not affected **2003:** not affected	04-029
Kernel and LSASS privilege elevation	Fixes vulnerabilities in kernel's launching of applications and LSASS validation of identity tokens which could allow a normal user to gain administrative access. (CVE 2004-0893 CVE 2004-0894)	**NT:** 885835 **2000:** 885835 or SP4 Update Rollup 1 **XP:** 885835 **2003:** 885835 or SP1	04-044
WordPad Word-for-Windows Converter buffer overflow	Fixes buffer overflows in table conversion and font conversion which could allow command execution when a malformed document is opened in WordPad. (CVE 2004-0571 CVE 2004-0901)	**NT:** 885836 **2000:** 885836 or SP4 Update Rollup 1 **XP:** 885836 **2003:** 885836 or SP1	04-041
Windows HyperTerminal buffer overflow	Fixes a vulnerability which could allow code execution when a user opens a malicious `.ht` file or possibly a Telnet URL. (CVE 2004-0568)	**NT:** 873339 **2000:** 873339 or SP4 Update Rollup 1 **XP:** 873339 **2003:** 873339 or SP1	04-043
HTML Help cross-domain vulnerability	Fixes a vulnerability which could allow command execution in the *Local Machine* security zone when a user follows a specially crafted link. (CVE 2004-1043)	**NT:** 890175 **2000:** 890175 or SP4 Update Rollup 1 **XP:** 890175 **2003:** 890175 or SP1	05-001 TA05-012B Bugtraq
Cursor and Icon vulnerabilities	Fixes vulnerabilities allowing command execution or a system crash when a user opens a malformed cursor or icon file. (CVE 2004-1049 CVE 2004-1305)	**NT:** 891711 **2000:** 891711 or SP4 Update Rollup 1 **XP:** 891711 or SP2 **2003:** 891711 or SP1	05-002 TA05-012A
Indexing service buffer overflow	Fixes a command execution vulnerability exploitable by an authenticated user, or by a web user if IIS allows access to indexing. (CVE 2004-0897)	**2000:** 871250 or SP4 Update Rollup 1 **XP:** 871250 or SP2 **2003:** 871250 or SP1	05-003
DHTML Editing Component vulnerability	Fixes a cross-domain vulnerability allowing information disclosure or command execution when a user visits	**2000:** 891781 or SP4 Update Rollup 1	05-013

	a malicious web page. (CVE 2004-1319)	**XP:** 891781 **2003:** 891781 or SP1	
Hyperlink Object Library buffer overflow	Fixes a buffer overflow which could allow command execution when a user clicks on a specially crafted hyperlink. (CVE 2005-0057)	**2000:** 888113 or SP4 Update Rollup 1 **XP:** 888113 **2003:** 888113 or SP1	05-015
OLE and COM vulnerabilities	Fixes two vulnerabilities, the more critical of which could allow command execution by a malicious document. (CVE 2005-0044 CVE 2005-0047)	**2000:** 873333 or SP4 Update Rollup 1 **XP:** 873333 **2003:** 873333 or SP1	05-012
PNG Image Processing Vulnerability	Fixes a vulnerability which could allow command execution when Windows Media Player or Windows Messenger opens a malformed image. (CVE 2004-0597 CVE 2004-1244)	**Media Player 9:** 885492 **Windows Messenger:** 5.1	05-009
Named Pipe Information Disclosure	Prevents attackers from reading the names of users who are connected to shared resources. (CVE 2005-0051)	**2000:** Not affected **XP:** 888302 or disable Computer Browser service **2003:** Not affected	05-007
Windows Shell Drag-and-Drop Vulnerability	Fixes a vulnerability which could allow writing of arbitrary files when a user takes certain actions on a malicious web page. (CVE 2005-0053)	**2000:** 890047 or SP4 Update Rollup 1 **XP:** 890047 **2003:** 890047 or SP1	05-008
SMB Transaction response buffer overflow	Fixes command execution vulnerability in processing of responses to Transaction commands by the SMB client driver. (CVE 2005-0045)	**2000:** 885250 or SP4 Update Rollup 1 **XP:** 885250 **2003:** 885250 or SP1	05-011
Windows XP Unprivileged Remote Shutdown	Fixes Windows XP SP1 Remote Desktop to observe the *Force shutdown from a remote system* user right when running **`TSShutdn.exe`**. (CVE 2005-0904)	**2000:** Not affected **XP:** SP2 or 889323 **2003:** Not affected	889323
Windows TCP/IP Vulnerabilities	Fixes vulnerabilities which could allow a remote attacker to cause a denial of service, or possibly execute commands. (CVE 2004-0230 CVE 2004-0790 CVE 2004-1060 CVE 2005-0048 CVE 2005-0688)	**2000:** 893066 or SP4 Update Rollup 1 **XP:** 893066 **2003:** 893066 or SP1	05-019
HTML Application Host vulnerability in Windows shell	Fixes a vulnerability which could allow an e-mail attachment of an unregistered type to execute code using HTML Application Host. (CVE 2005-0063)	**2000:** 893086 or SP4 Update Rollup 1 **XP:** 893086 **2003:** 893086 or SP1	05-016
Windows kernel access request buffer overflow	Fixes vulnerabilities in the Windows kernel which could allow privilege elevation or denial of service. (CVE 2005-0060 CVE 2005-0061 CVE	**2000:** 890859 or SP4 Update Rollup 1 **XP:** 890859	05-018

	2005-0550 CVE 2005-0551)	**2003:** 890859 or SP1	
Message Queuing vulnerability	Fixes a buffer overflow in Message Queuing which could allow remote command execution. (Sites using only HTTP Message Delivery are not affected.) (CVE 2005-0059)	**2000:** 892944 or SP4 Update Rollup 1 **XP:** 892944 or SP2 **2003:** not affected	05-017
Jet Database Engine input validation	Fixes vulnerabilities which could allow command execution by a malformed database file. (CVE 2005-0944)	**2000:** 950749 **XP:** 950749 **2003 SP1:** 950749	08-028 VU#936529 Full Disclosure
Windows Explorer Web View	Fixes vulnerability which could allow a malicious file to execute commands when previewed in Windows Explorer's Web View. (CVE 2005-1191)	**2000:** 894320 **XP:** Not affected **2003:** Not affected	05-024 Bugtraq
HTML Help integer overflow	Fixes an integer overflow in HTML Help which could allow command execution. (CVE 2005-1208)	**2000:** 896358 **XP:** 896358 **2003:** 896358 or SP2	05-026 VulnWatch
Interactive Training bookmark file buffer overflow	Fixes a vulnerability which allows command execution when a user opens a **.cbo** file with a long User field. (CVE 2005-1212)	898458	05-031 BugTraq ID 13944
Microsoft Agent spoofing vulnerability	Prevents spoofing of trusted Internet content using a Microsoft Agent character which disguises security prompts. (CVE 2005-1214)	**2000:** 890046 **XP:** 890046 **2003:** 890046 or SP2	05-032
SMB input validation vulnerability	Fixes a vulnerability which could allow remote code execution. (CVE 2005-1206)	**2000:** 896422 **XP:** 896422 **2003:** 896422 or SP2	05-027
Telnet client session variable disclosure	Fixes a vulnerability which could reveal telnet session variables to an attacker when a user clicks on a malformed telnet URL. (CVE 2005-1205)	**XP:** 896428 **2003:** 896428 or SP2 **Services for UNIX 3.5:** 896428 **Services for UNIX 3.0:** 896428 **Services for UNIX 2.2:** 896428	05-033
Microsoft Color Management Module buffer overflow	Fixes a vulnerability in ICC profile format tag validation which could allow command execution when a user views a malformed image. (CVE 2005-1219)	**2000:** 901214 **XP:** 901214 **2003:** 901214 or SP2	05-036
Windows 2000 SP4 Update Rollup 1	Update Rollup 1 for Windows 2000 SP4 fixes multiple potential problems. (CVE 2005-3168 CVE 2005-3169 CVE 2005-3170 CVE 2005-3171 CVE 2005-3172 CVE 2005-3173 CVE 2005-3174 CVE 2005-3175 CVE 2005-3176 CVE 2005-3177)	**2000:** SP4 Update Rollup 1	SP4 Update Rollup 1
DirectShow Buffer Overflow	Fixes a vulnerability in DirectX which could allow command execution by a specially crafted **.avi** file. (CVE 2005-2128)	**2000:** 904706 **XP:** 904706 **2003:** 904706 or SP2	05-050
Windows COM+ command execution	Fixes vulnerabilities which could allow	**2000:** 902400	05-051

vulnerability	remote command execution on Windows 2000 and XP SP1, or privilege elevation on Windows XP SP2 and 2003. (CVE 2005-1978 CVE 2005-1979 CVE 2005-1980 CVE 2005-2119)	**XP:** 902400 **2003:** 902400 or SP2	
Windows Shortcut File command execution	Fixes three Windows shell vulnerabilities, the most critical of which could allow command execution when a **.lnk** file is opened. (CVE 2005-2117 CVE 2005-2118 CVE 2005-2122)	**2000:** 900725 **XP:** 900725 **2003:** 900725 or SP2	05-049
Collaboration Data Object vulnerability	Fixes a vulnerability in Collaboration Data Objects which could allow an attacker to perform remote code execution. (CVE 2005-1987)	**2000:** 901017 **XP:** 901017 **2003:** 901017 or SP2	05-048
Client Service for NetWare vulnerability	Fixes a vulnerability in Client Service for NetWare which could allow an attacker to perform remote code execution. (CVE 2005-1985)	**2000:** 899589 **XP:** 899589 **2003:** 899589	05-046
FTP Client vulnerability	Fixes a vulnerability in Windows FTP Client that could allow tampering in File Transfer location. (CVE 2005-2126)	**2000:** 905495 **XP:** 905495 **2003:** 905495	05-044
Network Connection Manager vulnerability	Fixes a vulnerability in Network Connection Manager that could allow Denial of Service. (CVE 2005-2307)	**2000:** 905414 **XP:** 905414 **2003:** 905414 or SP2	05-045
Windows EMF/WMF image file vulnerability	Fixes a vulnerability in the graphics engine processing of EMF/WMF image files that could allow an attacker to take control of a host. (CVE 2005-0803 CVE 2005-2123 CVE 2005-2124)	**2000:** 896424 **XP:** 896424 **2003:** 896424 or SP2	05-053
Windows Kernel privilege elevation vulnerability	Fixes a vulnerability in the Windows 2000 Kernel that allows an attacker *who has successfully logged into the system* to take control of a host. (CVE 2005-2827)	**2000:** 908523	05-055
Windows WMF gdi32.dll vulnerability	Fixes a remote code execution vulnerability which exists in the Graphics Rendering Engine because of the way that it handles Windows Metafile (WMF) images. An attacker could exploit the vulnerability to take complete control of the affected system by constructing a specially crafted WMF image which is read by a user on the system. (CVE 2005-4560)	**2000:** 912919 **XP:** 912919 **2003:** 912919 or SP2	06-001
Windows web fonts vulnerability	Fixes a vulnerability in embedded web fonts that could allow remote code execution. An attacker could exploit the vulnerability by having a user access a web page with the malformed web fonts in it. This would allow the attacker to execute commands with the authority of the user. (CVE 2006-0010)	**2000:** 908519 **XP:** 908519 **2003:** 908519 or SP2	06-002
Windows Media Player bmp buffer overflow	Fixes a command execution vulnerability in bmp image parsing. (CVE 2006-0006)	911565	06-005

Windows Media Player plug-in EMBED vulnerability	Fixes a buffer overflow which could allow command execution when a user plays media files through non-Microsoft browsers. (CVE 2006-0005)	911564	06-006
Windows IGMP v3 DoS vulnerability	Fixes a denial-of-service vulnerability that would allow an attacker to send a specially crafted IGMP packet to an affected system causing the affected system to stop responding. (CVE 2006-0021)	**2000:** not affected **XP:** 913446 **2003:** 913446 or SP2	06-007
WebClient buffer overflow	Fixes a buffer overflow which could allow a remote authenticated user to gain administrative privileges. (CVE 2005-1207 CVE 2006-0013)	**2000:** not affected **XP:** 911927 **2003:** 911927 or SP2 or disable WebClient service	05-028 06-008
Korean IME privilege elevation vulnerability	Fixes a privilege elevation vulnerability which could allow an attacker who has interactively logged onto the system to take full control of the system. (CVE 2006-0008)	**2000:** not affected **XP:** 901190 **2003:** 901190	06-009
Windows DACL privilege elevation vulnerability	Fixes a privilege elevation vulnerability allowing full control of the system by any user on Windows XP or by a user in the network configuration operators group on Windows Server 2003. (CVE 2006-0023)	**2000:** not affected **XP:** 914798 or SP2 **2003:** 914798 or SP1	06-011
Windows Help File Image Processing Heap Buffer Overflow	Windows 2000, XP, and 2003 are affected by a heap overflow issue when handling a specially crafted Windows Help (.hlp) file containing a malicious image. (CVE 2006-1591)		Bugtraq ID 17325
Microsoft Data Access Component vulnerability	A remote code execution vulnerability exists in the RDS.Dataspace ActiveX control in ADO distributed in MDAC. Opening a file provided by an attacker (Mail or Website) allows an attacker to execute code with the rights of that user. (CVE 2006-0003)	**2000:** 911562 **XP:** 911562 **2003:** 911562 or SP2	06-014
Windows Explorer COM object command execution	Fixes a vulnerability which could allow command execution by a web site which forces a connection to a remote file server. (CVE 2004-2289 CVE 2006-0012)	**2000:** 908531 **XP:** 908531 **2003:** 908531 or SP2	06-015
Distributed Transaction Coordinator Denial of Service	Fixes two vulnerabilities that an attacker could use to cause the Microsoft Distributed Transaction Coordinator (MSDTC) to stop responding. (CVE 2006-0034 CVE 2006-1184)	**2000:** 913580 **XP:** 913580 **2003:** 913580	06-018
ART Rendering Buffer Overflow	Fixes a vulnerability which allows code execution when a user views a malformed ART image. (CVE 2006-2378)	**XP SP1/IE6:** 918439 **XP SP2:** 918439 **2003:** 918439 or SP2 **IE 5.01:** 918439	06-022
Routing and Remote Access Service remote code execution	Fixes a vulnerability that allows for remote code execution when the	**2000:** 911280 **XP:** 911280	06-025

	RASMAN service is active (CVE 2006-2370 CVE 2006-2371)	**2003:** 911280 or SP2	
Windows Media Player PNG buffer overflow	Fixes a vulnerability in Windows Media Player which could allow command execution when a user opens a malformed media file. (CVE 2006-0025)	917734	06-024
Windows SMB invalid handle denial of service	Fixes two vulnerabilities, one that would allow for a denial of service and the other which would allow privilege elevation. (CVE 2006-2373 CVE 2006-2374)	**2000:** 914389 **XP:** 914389 **2003:** 914389 or SP2	06-030
Windows TCP/IP remote code execution vulnerability	Fixes vulnerability in Windows TCP/IP IP Source Routing code which allows for remote code execution. (CVE 2006-2379)	**2000:** 917953 **XP:** 917953 **2003:** 917953 or SP2	06-032
Windows RPC Mutual Authentication spoofing	Fixes vulnerability in Windows RPC for Windows 2000 that allows for spoofing of RPC authentication. (CVE 2006-2380)	**2000:** 917736	06-031
Windows Mailslot Heap Overflow	Fixes a heap overflow in Mailslot allowing remote command execution, and an SMB information disclosure vulnerability. (CVE 2006-1314 CVE 2006-1315)	**2000:** 917159 **XP:** 917159 **2003:** 917159 or SP2	06-035
DHCP Client Buffer Overflow	Fixes a vulnerability which could allow command execution by an attacker-controlled DHCP server on the local subnet. (CVE 2006-2372)	**2000:** 914388 **XP:** 914388 **2003:** 914388 or SP2	06-036
Server Service Buffer Overrun	Fixes a vulnerability which could allow command execution on a buffer overrun on the Server Service (CVE 2006-3439)	**2000:** 921883 **XP:** 921883 **2003:** 921883 or SP2	06-040
DNS Resolution Remote Code Execution	Fixes vulnerabilities in the Winsock Hostname functionality and a DNS Resolution Client Buffer Overrun. (CVE 2006-3440 CVE 2006-3441)	**2000:** 920683 **XP:** 920683 **2003:** 920683 or SP2	06-041
Windows MMC redirect cross-site scripting vulnerability	Fixes vulnerabilities which allow for Remote Code Execution in the Microsoft Management Console on the load of malformed files. (CVE 2006-3643)	**2000:** 917008	06-044
Windows Explorer Folder GUID Code Execution vulnerability	Fixes a remote code execution vulnerability which exists in Windows Explorer dealing with Drag and Drop events. (CVE 2006-3281)	**2000:** 921398 **XP:** 921398 **2003:** 921398 or SP2	06-045
HTML Help ActiveX Control string buffer overflow	Fixes an overflow in a string buffer which could allow command execution by a malicious web site or e-mail. (CVE 2006-3357)	**2000:** 922616 **XP:** 922616 **2003:** 922616 or SP2	06-046
Windows Kernel privilege elevation vulnerability	Fixes a vulnerability that allows an attacker *who has successfully logged into the system* to take control of a host. Note: Different than MS05-055. (CVE 2006-3444)	**2000:** 920958	06-049
Hyperlink Object Library function vulnerability and buffer overflow	Fixes both a function vulnerability and a buffer overflow, either of which could allow command execution when a user	**2000:** 920670 **XP:** 920670 **2003:** 920670 or	06-050

	clicks on a specially crafted hyperlink. (CVE 2006-3086 CVE 2006-3438)	SP2	
Windows unhandled exception vulnerability	Fixes two vulnerabilities, including a bug in handling of chained exceptions allowing command execution when a user visits a malformed web page. (CVE 2006-3443 CVE 2006-3648)	**2000:** 917422 **XP:** 917422 **2003:** 917422 or SP2	06-051
Windows PGM remote code execution	Fixes a vulnerability which allows a malformed Pragmatic General Multicast (PGM) message to cause remote code execution through the MSMQ service. (CVE 2006-3442)	**2000:** not affected **XP:** 919007 **2003:** not affected	06-052
Windows PGM to Address Elevation of Privilege	This fixes a vulnerability which allows Elevation of Privilege if an attacker runs a specially crafted application that results in references to memory locations that have been freed. MSMQ must be installed, and Windows PGM protocol enabled for the system to be vulnerable.(CVE 2015-6126)	**Vista:** 3109103 (32-bit) 3109103 (64-bit) **2008:** 3109103 (32-bit) 3109103 (64-bit) **7:** 3109103 (32-bit) 3109103 (64-bit) **2008 R2:** 3109103 **8:** 3109103 (32-bit) 3109103 (64-bit) **8.1:** 3109103 (32-bit) 3109103 (64-bit) **2012:** 3109103 (32-bit) **2012 R2:** 3109103 (32-bit) **10:** 3116869 **10 v1511:** 3116900	15-133
Windows indexing service cross-site scripting	Fixes a vulnerability that allows cross-site scripting leading to information disclosure through the indexing (cisvc) service. (CVE 2006-0032)	**2000:** 920685 **XP:** 920685 **2003:** 920685 or SP2	06-053
Windows Explorer setslice remote code execution	Fixes a remote code execution vulnerability which exists in Windows Explorer WebViewFolderIcon ActiveX setslice function. A crafted website or email message could cause remote code execution. (CVE 2006-3730)	**2000:** 923191 **XP:** 923191 **2003:** 923191 or SP2	06-057
Microsoft XML Core Services remote code execution	Fixes two vulnerabilities in the XML Core services, a remote code execution and an information disclosure. (CVE 2006-4685 CVE 2006-4686)	924191	06-061
Windows SMB Remote Code Execution	Fixes a vulnerability in Microsoft Server Message Block (SMB) Protocol. The vulnerability could allow remote code execution on a server that is sharing files or folders. An attacker who successfully exploited this vulnerability could install programs; view, change, or delete data; or create new accounts	**2000:** 957095 **XP:** 957095 **2003:** 957095 **Vista:** 957095 **2008:** 957095	08-063 06-063

	with full user rights. (CVE 2008-4038) Also fixes other two vulnerabilities. A null pointer dereference in **`srv.sys`** allows an attacker to remotely crash the system. A validated attacker can execute code as administrator. (CVE 2006-3942 CVE 2006-4696)		
Windows TCP/IP IPv6 denial of service	Fixes vulnerabilities which allow for denial of service when IPv6 is used. (CVE 2004-0230, CVE 2004-0790, CVE 2005-0688, CVE 2005-1649)	**XP:** 922819 **2003:** 922819 or SP2	06-064
Windows Object Packer dialogue spoofing vulnerability	Fixes a vulnerability which could allow a file to execute commands by creating a misleading dialogue box. (CVE 2006-4692)	**XP:** 924496 **2003:** 924496 or SP2	06-065
Microsoft Windows NAT Helper DNS Query Denial of Service	DoS vulnerability in Windows NAT Helper caused by improper processing of crafted DNS queries. (CVE 2006-5614)		Bugtraq ID 20804
Client Service for NetWare buffer overflow and driver denial of service	Vulnerabilities allowing remote attacker to execute arbitrary commands or crash the system. (Requires valid login on 2003.) (CVE 2006-4688 CVE 2006-4689)	**2000:** 923980 **XP:** 923980 **2003:** 923980	06-066
Microsoft Agent ACF memory corruption	Microsoft Agent vulnerability causing remote code execution through read of crafted .ACF files read in web page. (CVE 2006-3445)	**2000:** 920213 **XP:** 920213 **2003:** 920213	06-068
Windows Workstation service remote code execution	A remote code execution vulnerability in Workstation service allows complete control of the affected system. (Note, administrator privileges are required for XP.) (CVE 2006-4691)	**2000:** 924270 **XP:** 924270 **2003:** Not affected	06-070
Microsoft XMLHTTP setRequestHeader code execution	XMLHTTP 4.0 and 6.0 ActiveX Control vulnerability in setRequestHeader allows remote code execution from read of crafted webpage. (CVE 2006-5745)	**MSXML 4.0:** 927978 **MSXML 6.0:** 927977	06-071
Client Server Run-Time Subsystem file manifest vulnerability	Fixes a vulnerability allowing local authenticated users to gain elevated privileges due to improper handling of file manifests. (CVE 2006-5585)	**XP:** 926255 **2003:** 926255	06-075
Windows Media Format ASX Parsing Buffer Overflow	Fixes vulnerabilities in Windows Media Format which could allow command execution when parsing ASF and ASX files. (CVE 2006-4702 CVE 2006-6134)	**2000:** 923689 or 925398 (WMP 6.4) **XP:** 923689 or 925398 (WMP 6.4) **2003:** 923689 or 925398 (WMP 6.4)	06-078
Microsoft Windows Workstation Service NetrWkstaUserEnum denial of service	Vulnerability in the Workstation Service that allows for a temporary denial of service due to memory allocation. (CVE 2006-6723)	Not currently fixed	Secunia Advisory SA23487
HTML Help ActiveX Control remote code execution	Fixes an overflow which could allow command execution by a malicious web site or e-mail. (CVE 2007-0214)	**2000:** 928843 **XP:** 928843 **2003:** 928843	07-008
Interactive Training bookmark file remote code execution	Fixes a vulnerability which allows command execution when a user opens a bookmark file. (CVE	923723	07-005

	2006-3448)		
Windows Shell Privilege Elevation	Fixes a privilege elevation vulnerability when Shell Hardware Detection service is enabled. (CVE 2007-0211)	**XP:** 928843 **2003:** 928843	07-006
Windows Image Acquisition Privilege Elevation	Fixes a privilege elevation vulnerability when the Windows Image Acquisition (WIA) service (stisvc) is enabled. (CVE 2007-0210)	**XP:** 927802	07-007
RTF OLE dialog memory corruption	Fixes a memory corruption of OLE objects within RTF files. (CVE 2007-0026)	**2000:** 926436 **XP:** 926436 **2003:** 926436	07-011
RTF MFC component memory corruption	Fixes a memory corruption of MFC components within RTF files. (CVE 2007-0025)	**2000:** 924667 **XP:** 924667 **2003:** 924667	07-012
RTF RichEdit component memory corruption	Fixes a memory corruption of RichEdit components within RTF files. (CVE 2006-1311)	**2000:** 918118 **XP:** 918118 **2003:** 918118	07-013
Microsoft Malware Protection Engine PDF integer overflow	Fixes an integer overflow which can occur when the Malware Protection Engine processes PDF files. (CVE 2006-5270)	Automatic update from Microsoft Update, Windows Live OneCare AutoUpdate, or Forefront Server security update service	07-010
Multiple GDI vulnerabilities fixed by MS07-017	Multiple vulnerabilities in parts of the Graphic Design Interface including remote code execution. (CVE 2006-5586 CVE 2006-5758 CVE 2007-0038 CVE 2007-1211 CVE 2007-1212 CVE 2007-1213 CVE 2007-1215)	**2000:** 925902 **XP:** 925902 **2003:** 925902 **Vista:** 925902	07-017
Windows Kernel privilege elevation vulnerability	Fixes a vulnerability that allows an attacker *who has successfully logged into the system* to take control of a host. Note: Different than MS05-055 and MS06-049. (CVE 2007-1206)	**2000:** 931784 **XP:** 931784 **2003:** 931784	07-022
Windows CSRSS remote code execution	Fixes vulnerabilities in the Windows Client/Server Run-time Subsystem (CSRSS) that include remote code execution. (CVE 2006-6696 CVE 2006-6797 CVE 2007-1209)	**2000:** 930178 **XP:** 930178 **2003:** 930178 **Vista:** 930178	07-021
Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege	Fixes a vulnerability which could allow elevation of privilege if an attacker logged on to an affected system that is configured with a Chinese, Japanese, or Korean system locale. An attacker who successfully exploited this vulnerability could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE 2010-1891)	**XP:** KB2121546 **2003:** KB2121546	10-069
Microsoft Agent URL parsing vulnerability	Fixes a vulnerability in Microsoft Agent that allows remote code execution when reading a crafted URL (CVE 2007-1205)	**2000:** 932168 **XP:** 932168 **2003:** 932168	07-020
Windows Help File Handling Heap Buffer Overflow	Windows 2000, XP, and 2003 are affected by a heap overflow issue		Bugtraq ID 23382

	when handling a specially crafted Windows Help (.hlp) file containing a malicious bitmap. (CVE 2007-1912)		
CAPICOM.Certificates ActiveX control code execution	Fixes a vulnerability in the Cryptographic API Component Object Model (CAPICOM) allowing code execution by a malicious web page. (CVE 2007-0940)	931906	07-028
Windows DirectX ActiveX control Denial of Service	Internet Explorer Denial of Service in the DirectX Media software for XP. (CVE 2006-4301)		Bugtraq archive 443901
Windows Schannel digital signature parsing vulnerability	Fixes a vulnerability affecting applications which use SSL/TLS allowing code execution on Windows XP and denial of service on Windows 2000 and 2003. (CVE 2007-2218)	**2000:** 935840 **XP:** 935840 **2003:** 935840	07-031
Vulnerability in TLS Could Disclose Information	Fixes a vulnerability which could allow information disclosure if an attacker intercepts encrypted web traffic served from an affected system. (CVE 2012-1870)	**XP:**2655992 (32-bit), 2655992 (64-bit) **2003:**2655992 (32-bit), 2655992 (64-bit) **Vista:**2655992 (32-bit), 2655992 (64-bit) **2008:**2655992 (32-bit), 2655992 (64-bit) **Win 7:**2655992 (32-bit), 2655992 (64-bit) **2008 R2:**2655992 (64-bit)	12-049
Fixes Vista Permissive User Information Store ACLs Information Disclosure Vulnerability	Fixes a vulnerability allowing non-privileged users to access local user information data stores such as admin passwords contained within the registry and local file system. (CVE 2007-2229)	**Vista:** 931213	07-032
Win32 API parameter validation vulnerability	Fixes a vulnerability which could allow command execution by a specially crafted web site. (CVE 2007-2219)	**2000:** 935839 **XP:** 935839 **2003:** 935839	07-035
GDI+ component ICO divide by zero	Fixes a divide by zero error in the Graphics Device Interface which could allow denial of service when an application opens a malformed image. Affects Windows 2003. (CVE 2007-2237)	Do not download ICO files from untrusted sources.	VU#290961
Windows Vista Teredo interface firewall bypass	Fixes a flaw which could allow network traffic to bypass firewall rules on the Teredo interface. (CVE 2007-3038)	**Vista:** 935807	07-038
DirectX RLE Compressed Targa Image File Heap Overflow	Fixes a buffer overflow vulnerability in DirectX libraries which handles compressed Targa (TGA) files. (CVE 2006-4183)	Update to the October 2006 version of DirectX or later.	Secunia Advisory SA26131
Microsoft XML Core Services remote code execution	Fixes a vulnerability in the XML Core services which allowed for remote code execution on processing of a	**Windows XP Service Pack 3, Microsoft XML**	07-042 08-069 10-051

crafted file. (CVE 2007-2223) Fixes a vulnerability in Microsoft XML Core Services 3.0 which allows command execution when a user loads a specially crafted HTML page. (CVE 2010-2561) Fixes multiple vulnerabilities which could allow code execution when XML content is parsed. (CVE 2007-0099 CVE 2008-4029 CVE 2008-4033) Fixes a vulnerability in the XML Core services which allowed for remote code execution if a user views a specially crafted webpage using Internet Explorer. (CVE 2012-1889 CVE 2013-0006 CVE 2013-0007)	Core Services 4.0:KB2758694 **Windows XP Service Pack 3, Microsoft XML Core Services 6.0:**KB2757638 **Windows XP Professional x64 Edition Service Pack 2, Microsoft XML Core Services 3.0:**KB2757638 **Windows XP Professional x64 Edition Service Pack 2, Microsoft XML Core Services 4.0:**KB2758694 **Windows XP Professional x64 Edition Service Pack 2, Microsoft XML Core Services 6.0:**KB2758696 **Windows Server 2003 Service Pack 2, Microsoft XML Core Services 4.0:**KB2758694 **Windows Server 2003 Service Pack 2, Microsoft XML Core Services 6.0:**KB2758696 **Windows Server 2003 x64 Edition Service Pack 2, Microsoft XML Core Services 3.0:**KB2757638 **Windows Server 2003 x64 Edition Service Pack 2, Microsoft XML Core Services 4.0:**KB2758694 **Windows Server 2003 x64 Edition Service Pack 2, Microsoft XML Core Services 6.0:**KB2758696	12-043 13-002 (KB2758696 is superseded by 14-033 for Windows Server 2003)

Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft XML Core Services 3.0:KB2757638
Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft XML Core Services 4.0:KB2758694
Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft XML Core Services 6.0:KB2758696
Windows Vista Service Pack 2, Microsoft XML Core Services 4.0:KB2758694
Windows Vista Service Pack 2, Microsoft XML Core Services 6.0:KB2757638
Windows Vista x64 Edition Service Pack 2, Microsoft XML Core Services 3.0:KB2757638
Windows Vista x64 Edition Service Pack 2, Microsoft XML Core Services 4.0:KB2758694
Windows Vista x64 Edition Service Pack 2, Microsoft XML Core Services 6.0:KB2757638
Windows Server 2008 for 32-bit Systems Service Pack 2, Microsoft XML Core Services 4.0:KB2758694
Windows Server 2008 for 32-bit

Systems Service Pack 2, Microsoft XML Core Services 6.0:KB2757638
Windows Server 2008 for x64-based Systems Service Pack 2, Microsoft XML Core Services 3.0:KB2757638
Windows Server 2008 for x64-based Systems Service Pack 2, Microsoft XML Core Services 4.0:KB2758694
Windows Server 2008 for x64-based Systems Service Pack 2, Microsoft XML Core Services 6.0:KB2757638
Windows Server 2008 for Itanium-based Systems Service Pack 2, Microsoft XML Core Services 3.0:KB2757638
Windows Server 2008 for Itanium-based Systems Service Pack 2, Microsoft XML Core Services 4.0:KB2758694
Windows Server 2008 for Itanium-based Systems Service Pack 2, Microsoft XML Core Services 6.0:KB2757638
Windows 7 for 32-bit Systems, Microsoft XML Core Services 4.0:KB2758694

Windows 7 for 32-bit Systems, Microsoft XML Core Services 6.0:KB2757638
Windows 7 for 32-bit Systems Service Pack 1, Microsoft XML Core Services 4.0:KB2758694
Windows 7 for 32-bit Systems Service Pack 1, Microsoft XML Core Services 6.0:KB2757638
Windows 7 for x64-based Systems, Microsoft XML Core Services 3.0:KB2757638
Windows 7 for x64-based Systems, Microsoft XML Core Services 4.0:KB2758694
Windows 7 for x64-based Systems, Microsoft XML Core Services 6.0:KB2757638
Windows 7 for x64-based Systems Service Pack 1, Microsoft XML Core Services 3.0:KB2757638
Windows 7 for x64-based Systems Service Pack 1, Microsoft XML Core Services 4.0:KB2758694
Windows 7 for x64-based Systems Service Pack 1, Microsoft XML Core Services 6.0:KB2757638
Windows Server 2008 R2 for

x64-based Systems, Microsoft XML Core Services 3.0:KB2757638
Windows Server 2008 R2 for x64-based Systems, Microsoft XML Core Services 4.0:KB2758694
Windows Server 2008 R2 for x64-based Systems, Microsoft XML Core Services 6.0:KB2757638
Windows Server 2008 R2 for x64-based Systems Service Pack 1, Microsoft XML Core Services 3.0:KB2757638
Windows Server 2008 R2 for x64-based Systems Service Pack 1, Microsoft XML Core Services 4.0:KB2758694
Windows Server 2008 R2 for x64-based Systems Service Pack 1, Microsoft XML Core Services 6.0:KB2757638
Windows Server 2008 R2 for Itanium-based Systems, Microsoft XML Core Services 3.0:KB2757638
Windows Server 2008 R2 for Itanium-based Systems, Microsoft XML Core Services 4.0:KB2758694
Windows Server

2008 R2 for Itanium-based Systems, Microsoft XML Core Services 6.0:KB2757638
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1, Microsoft XML Core Services 3.0:KB2757638
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1, Microsoft XML Core Services 4.0:KB2758694
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1, Microsoft XML Core Services 6.0:KB2757638
Windows 8 for 32-bit Systems, Microsoft XML Core Services 4.0:KB2758694
Windows 8 for 32-bit Systems, Microsoft XML Core Services 6.0:KB2757638
Windows 8 for 64-bit Systems, Microsoft XML Core Services 3.0:KB2757638
Windows 8 for 64-bit Systems, Microsoft XML Core Services 4.0:KB2758694
Windows 8 for 64-bit Systems, Microsoft XML Core Services 6.0:KB2757638
Windows Server 2012, Microsoft XML Core

		Services 3.0:KB2757638 **Windows Server 2012, Microsoft XML Core Services 4.0:**KB2758694 **Windows Server 2012, Microsoft XML Core Services 6.0:**KB2757638	
Windows OLE Automation remote code execution	Fixes a vulnerability in the OLE automation which allowed for remote code execution on processing of a crafted file. (CVE 2007-2224)	**2000:** 921503 **XP:** 921503 **2003:** 921503	07-043
Windows GDI image handling buffer overflow	Fixes a vulnerability in the Windows graphics device interface allowing command execution when a specially crafted image is rendered. (CVE 2007-3034)	**2000:** 938829 **XP:** 938829 **2003:** 938829	07-046
Windows Media Player Skin parsing and decompression remote code execution	Fixes a vulnerability in Windows Media Player which could allow command execution when a user opens a media file with a malformed skin. (CVE 2007-3035 CVE 2007-3037)	936782	07-047
Windows Gadgets remote code execution vulnerabilities	Fixes vulnerabilities in Windows Gadgets for Headline, Contacts and Weather that allow for remote code execution when accessing remote feeds. (CVE 2007-3032 CVE 2007-3033 CVE 2007-3891)	**Vista:** 938123	07-048
DirectX DirectTransform FlashPix ActiveX buffer overflow	Fixes a remote code execution vulnerability in the DirectTransform FlashPix ActiveX control as packaged in Microsoft DirectX Media 6.0 SDK. (CVE 2007-4336)	Workaround: Set kill bit for CLSID 201EA564-A6F6-11D1-811D-00C04FB6BD36.	Secunia Advisory SA26426
Microsoft Agent ActiveX remote code execution	Fixes an additional vulnerability in Microsoft Agent that allows remote code execution when reading a crafted URL. (CVE 2007-3040)	**2000:** 938827	07-051
Windows Services for UNIX 3.0 and 3.5, and Subsystem for UNIX-based Applications setuid privilege elevation	Fixes a vulnerability in Windows Services for UNIX where running certain setuid binary files could allow an attacker to gain elevated privileges. (CVE 2007-3036)	**WS UNIX 3.0:** 939778 **WS UNIX 3.5:** 938827 **SfUA 2003:** 938827 **SfUA Vista:** 938827	07-053
Vulnerable MFC Library FileFind Class file Heap Overflow	A Heap Overflow exists in the Microsoft Windows MFC Shared Library - FileFind Class. (CVE 2007-4916)	**XP:** 2387149 **2003:** 2387149	VU#611008 SA26800
Kodak Image Viewer remote code execution	Fixes a vulnerability in the Kodak Image Viewer that allows for remote code execution when viewing a crafted file. (CVE 2007-2217)	**2000:** 923810 **XP:** 923810 **2003:** 923810	07-055

Windows RPC Authentication denial of service	Fixes vulnerability in Windows RPC for Windows that allows for a denial of service to be caused in the RPC authentication. (CVE 2007-2228)	**2000:** 933729 **XP:** 933729 **2003:** 933729 **Vista:** 933729	07-058
SharePoint Services site privilege elevation	SharePoint Services 3.0 and Office SharePoint Server 2007 have an elevation of privilege vulnerability within the SharePoint site. (CVE 2007-2581)	**2003 SharePoint Services 3.0:** 934525 **Office SharePoint Server 2007:** 934525, and 937832	07-059
Microsoft SharePoint Server 2007 Elevation of Privilege	Microsoft SharePoint Server 2007 has an elevation of privilege vulnerability within the SharePoint site. (CVE 2008-3006)	**Microsoft SharePoint Server 2007:** KB953397	08-043
Shell32.dll Windows URI handling Remote Code Execution	Fixes vulnerability in Windows URI handling that can lead to remote code execution. (CVE 2007-3896)	**XP:** 943460 **2003:** 943460	07-061
Jet Database Engine vulnerable version	Fixes a vulnerability which could allow an attacker to execute arbitrary code by enticing a target user to open a crafted MDB file. (CVE 2007-6026 CVE 2008-1092)	**2000:** 950749 **XP:** 950749 **2003 SP1:** 950749	08-028 VU#936529
Windows Vista SMBv2 Remote Code Execution	Fixes a vulnerability that could allow an attacker to tamper with data transferred in SMBv2 leading to remote code execution. (CVE 2007-5351)	**Vista:** 942624	07-063
DirectX Parsing Remote Code Execution	Fixed vulnerabilities that could allow remote code execution parsing SAMI, WAV or AVI files. (CVE 2007-3895 CVE 2007-3901)	**2000 (7.0):** 941568 **2000 (8.0):** 941568 **2000 (9.0c):** 941568 **XP:** 941568 **2003:** 941568 **Vista:** 941568	07-064
Microsoft Video ActiveX Control Stack Buffer Overflow	A buffer overflow vulnerability exists in Microsoft DirectShow. The flaw is due to the way Microsoft Video ActiveX Control parses image files. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. (CVE 2008-0015)	**Video ActiveX Control:** 972890	09-032
Message Queuing validation vulnerability	Fixes a buffer overflow in Message Queuing which could allow remote command execution for Windows 2000 and privilege elevation for Windows XP. (CVE 2007-3039)	**2000:** 937894 **XP:** 937894	07-065
Vulnerability in Message Queuing Could Allow Elevation of Privilege	Fixes a memory corruption vulnerability in Message Queuing. The vulnerability is caused by a failure to validate messages containing user-defined memory address. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges. (CVE	**2000:** 971032 **XP:** 971032 **2003:** 971032 **Vista:** 971032	09-040 08-065

	2008-3479) Fixes a vulnerability in the Windows Message Queuing Service (MSMQ). The vulnerability could allow elevation of privilege if a user received a specially crafted request to an affected MSMQ service. (CVE 2009-1922)		
Windows Kernel privilege elevation vulnerability	Fixes a vulnerability that allows an attacker *who has successfully logged into the system* to take control of a host running Vista. (CVE 2007-5350)	**Vista:** 943078	07-066
Windows Media Format ASF file parsing vulnerability	Fixes a vulnerability allowing command execution when Windows Media Player or Media Services processes malformed content. (CVE 2007-0064)	**Windows Media Format:** 941569 **Windows Media Services:** 944275	07-068
Multiple Windows TCP/IP vulnerabilities	Fixes two vulnerabilities: (1) an IGMPv3 and MLDv2 vulnerability that could allow remote code execution; and (2) an ICMP vulnerability that could result in denial of service. (CVE 2007-0069, CVE 2007-0066)	**2000:** 941644 **XP:** 941644 **2003:** 941644 **Vista:** 941644	08-001
Windows LSASS vulnerability	Fixes a vulnerability that could allow an attacker to gain elevated privileges. (CVE 2007-5352)	**2000:** 943485 **XP:** 943485 **2003:** 943485	08-002
Vista DHCP response denial of service	Fixes a TCP/IP vulnerability allowing a denial of service by a response from a DHCP server. (CVE 2008-0084)	**Vista:** 946456	08-004
Windows WebDAV Mini-Redirector Remote Code Execution	Fixes a vulnerability that could allow a remote attacker to take complete control of an affected system. (CVE 2008-0080)	**XP:** 946026 **2003:** 946026 **Vista:** 946026	08-007
Windows OLE Automation Heap Overrun	Fixes a heap-based buffer overflow in Object Linking and Embedding (OLE) automation that could allow remote attackers to execute arbitrary code via a crafted request. (CVE 2007-0065)	**2000:** 943055 **XP:** 943055 **2003:** 943055 **Vista:** 943055	08-008
Windows DNS Spoofing Attack vulnerability	Fixes a vulnerability in the Windows DNS client that leads to a lack of entropy in the randomness of the choice of transaction IDs which could allow an attacker to send malicious responses to DNS requests. (CVE 2008-0087)	**2000:** 945553 **XP:** 945553 **2003:** 945553 **Vista:** 945553	08-020
Windows GDI remote code execution	Fixes several vulnerabilities: (1) stack overflow vulnerability in the way Graphics Device Interface (GDI) handles filename parameters in EMF image files; (CVE 2008-1087) (2) heap overflow vulnerability in the way GDI handles integer calculations; (CVE 2008-1083) (3) remote code execution vulnerability in the way that GDI handles integer calculations; (CVE 2008-2249) (4) remote code execution vulnerability in the way that GDI handles file size parameters in WMF files. (CVE 2008-3465)	Contact your vendor for the appropriate patch.	08-071 08-021

Windows kernel user mode callback vulnerability	Fixes a privilege elevation vulnerability caused by insufficient validation of input passed from user mode to the kernel. (CVE 2008-1084)	**2000:** 941693 **XP:** 941693 **2003:** 941693 **Vista:** 941693 **2008:** 941693	08-025
DirectX SAMI-MJPEG Parsing Remote Code Execution	Fixed vulnerabilities that could allow remote code execution parsing MJPEG and SAMI files. (CVE 2008-0011 CVE 2008-1444)	**2000:** 951698 **XP:** 951698 **2003:** 951698 **Vista:** 951698 **2008:** 951698	08-033
Windows PGM denial of service	Fixes two vulnerabilities which allow a malformed Pragmatic General Multicast (PGM) message to cause a denial of service through the MSMQ service. (CVE 2008-1440 CVE 2008-1441)	**2000:** not affected **XP:** 950762 **2003:** 950762 **Vista:** 950762 **2008:** 950762	08-036
Snapshot Viewer for Microsoft Access file download vulnerability	Fixes a vulnerability which could allow files to be downloaded to arbitrary locations. (CVE 2008-2463)	**Set kill bits** (see 08-041) **Snapshot Viewer 2000:** 955441 **Snapshot Viewer 2002:** 955440 **Snapshot Viewer 2003:** 955439	08-041
Windows DNS Client Spoofing vulnerability	Fixes a vulnerability in the Windows DNS client. This vulnerability could allow a remote unauthenticated attacker to quickly and reliably spoof responses and insert records into the client cache, thereby redirecting Internet traffic. (CVE 2008-1447)	**2000:** 951748 **XP:** 951748 **2003:** 951748	08-037
Windows DNS Server Spoofing vulnerability	Fixes two vulnerabilities in the Windows DNS Server. The vulnerabilities could allow spoofing by poisoning the DNS cache. (CVE 2008-1447 CVE 2008-1454)	**2000:** 951746 **2003:** 951746 **2008:** 951746	08-037
Windows Explorer Remote Code Execution	Fixes several vulnerabilities: (1) remote code execution vulnerability when a specially crafted saved-search file is opened and saved; (CVE 2008-1435) (2) remote code execution vulnerability when saving a specially crafted search file within Windows Explorer; (CVE 2008-4268) (3) remote code execution vulnerability in Windows Explorer that allows an attacker to construct a malicious web page that includes a call to the `search-ms` protocol handler. (CVE 2008-4269)	**Vista:** 958624 **2008:** 958624, 958623	08-075 08-038
Microsoft Image Color Management System vulnerable version	Fixes a vulnerability which could allow remote command execution on Windows 2000, Windows XP and Windows Server 2003. (CVE 2008-2245)	**2000:** 952954 **XP:** 952954 **2003:** 952954	08-046
Windows Messenger UIAutomation ActiveX vulnerability	Fixes an information disclosure vulnerability caused by an ActiveX control which is incorrectly marked safe. (CVE 2008-0082)	**XP:** 946648 **2003:** 954723	08-050

Event System vulnerabilities	Fixes two vulnerabilities which allow authenticated users to execute arbitrary code on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. (CVE 2008-1456 CVE 2008-1457)	**2000:** 950974 **XP:** 950974 **XP Professional x64:** 950974 **2003:** 950974 **2003 x64** 950974 **Vista:** 950974 **Vista x64:** 950974 **2008:** 950974 **2008 x64:** 950974	08-049
Active Directory Federation Services vulnerable version	Fixes two vulnerabilities which allow remote authenticated code execution and spoofing on Windows Server 2003 SP2, and Windows Server 2008. (CVE 2009-2508 CVE 2009-2509)	**2003 SP2:** 971726 **2003 SP2 x64:** 971726 **2008 & SP2:** 971726 **2008 x64 & SP2:** 971726	09-070
Windows kernel vulnerable version	Fixes multiple vulnerabilities which allow authenticated users to elevate privileges on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7. (CVE 2009-2515 CVE 2009-2516 CVE 2009-2517 CVE 2010-0232 CVE 2010-0233)	**2000:** 977165 **XP:** 977165 **2003:** 977165 **Vista:** 977165 **2008:** 977165 **Windows 7:** 977165	09-058 10-015
Windows GDI+ vulnerabilities	Fixes vulnerabilities in the gdiplus.dll of Microsoft Windows GDI+ subsystem which could allow remote code execution if a user viewed a specially crafted file. (CVE 2009-2500 CVE 2009-2501 CVE 2009-2502 CVE 2009-2503 CVE 2009-2504 CVE 2009-3126 CVE 2009-2528 CVE 2009-2518)	**XP:** 958869 **XP Professional x64:** 958869 **2003:** 958869 **2003 X64:** 958869 **2003 Itanium:** 958869 **Vista:** 958869 **Vista X64:** 958869 **2008:** 958869 **2008 X64:** 958869	09-062 (superseded by 11-029)
Windows GDI+ vulnerabilities	Fixes vulnerabilities in the gdiplus.dll of Microsoft Windows GDI+ subsystem which could allow remote code execution if a user viewed a specially crafted file. (CVE 2007-5348 CVE 2008-3012 CVE 2008-3013 CVE 2008-3014 CVE 2008-3015)	**XP:** 938464 **XP Professional x64:** 938464 **2003:** 938464 **2003 X64:** 938464 **Vista:** 938464 **Vista X64:** 938464 **2008:** 938464 **2008 X64:** 938464	08-052
Windows Media Player sampling rate vulnerability	Fixes a command execution vulnerability when streaming audio files from a Windows Media Server in a server-side playlist. (CVE 2008-2253)	**XP:** 954154 **Vista:** 954154 **2008:** 954154	08-054
Windows Media Encoder wmex.dll ActiveX vulnerability	Fixes a command execution vulnerability in an ActiveX control which was incorrectly marked safe-for-scripting. (CVE 2008-3008)	**2000:** 954156 **XP:** 954156 **2003:** 954156 **Vista:** 954156 **2008:** 954156	08-053
Windows kernel validation	Fixes vulnerabilities by validating input passed from user mode through the	**2000:** 958690 **XP:** 958690	09-006 08-061

	kernel component of GDI, correcting the way that the kernel validates handles, and changing the way that the Windows kernel handles specially crafted invalid pointers. (CVE 2009-0081 CVE 2009-0082 CVE 2009-0083) Fixes vulnerabilities by correcting window property validation passed during the new window creation process, calls from multiple threads are handled, and validation of parameters passed to the Windows Kernel from user mode. (CVE 2008-2250 CVE 2008-2251 CVE 2008-2252)	**2003:** 958690 **Vista:** 958690 **2008:** 958690	
AFD Kernel Overwrite vulnerability	Fixes a privilege elevation vulnerability in the Ancillary Function Driver which occurs when passing data from user to kernel mode. (CVE 2008-3464)	**XP:** 956803 **2003:** 956803	08-066
Elevation of Privilege Vulnerabilities in Windows	Fixes multiple privilege elevation vulnerabilities. (CVE 2008-4036 CVE 2008-1436 CVE 2009-0078 CVE 2009-0079 CVE 2009-0080)	**2000:** 952004 **XP:** 952004 **2003:** 952004 **Vista:** 952004 **2008:** 952004	08-064 09-012
Windows Server Service MS08-067 buffer overflow	Fixes a buffer overflow in the Windows Server service which could allow remote attackers to take complete control of the computer. (CVE 2008-4250)	**2000:** 958644 **XP:** 958644 **2003:** 958644 **Vista:** 958644 **2008:** 958644	08-067
Windows SMB credential reflection vulnerability	Fixes validation of NTLM authentication replies to ensure that a user's credentials are not reflected back to an attacker. (CVE 2008-4037)	**2000:** 957097 **XP:** 957097 **2003:** 957097 **Vista:** 957097 **2008:** 957097	08-068
Windows Media components SPN credential reflection vulnerability	Fixes a vulnerability which allows unauthorized access by forwarding a client's credentials and a credential disclosure vulnerability in ISATAP. (CVE 2008-3009 CVE 2008-3010)	**Media Player:** 954600 **Media Format:** 952069 **Media Services:** 952068	08-076
SharePoint Services site privilege elevation	Microsoft Office SharePoint Server 2007 and Microsoft Search Server 2008 have an elevation of privilege vulnerability within the SharePoint site. (CVE 2008-4032)	**Office SharePoint Server 2007:** 956716 (32 Bit) or 956716 (64 Bit) **Office Search Server 2008:** 956716 (32 Bit) or 956716 (64 Bit)	08-077
Microsoft SharePoint multiple vulnerabilities	Microsoft Office SharePoint Server 2007 to Microsoft Office SharePoint Server 2013 have multiple vulnerabilities. Exploitation of the most critical bug results in remote code execution. (CVE 2013-3889, CVE 2013-3895)	**Microsoft Office SharePoint Server 2007:** 2596741 (32 Bit) or 2596741 (64 Bit) **Microsoft Office SharePoint Server 2010:** 2589365	13-084

		Microsoft Office SharePoint Server 2013: 2827222 (wacserver) or 2760561 (pptserver) **Excel Services in Office SharePoint Server 2007:** 2827327 (32 Bit) or 2827327 (64 Bit) **Excel Services in Office SharePoint Server 2010:** 2826022 **Excel Services in Office SharePoint Server 2013:** 2752002 **Word Automation Services in Office SharePoint Server 2013:** 2826036	
Multiple Windows SMB vulnerabilities	Fixes multiple SMB buffer overflow vulnerabilities that could give an attacker administrative rights to the system. (CVE 2008-4114 CVE 2008-4834 CVE 2008-4835)	**2000:** 958687 (32 bit) **XP:** 958687 (32 bit) or 958687 (64 bit) **2003:** 958687 (32 bit), 958687 (64 bit), or 958687 Itanium **Vista:** 958687 (32 bit) or 958687 (64 bit) **2008:** 958687 (32 bit), 958687 (64 bit), or 958687 Itanium	09-001
Windows Schannel spoofing vulnerability	Fixes a spoofing vulnerability in windows 2000, 2003, XP, Vista, and 2008. The vulnerability is only harmful if the attacker gains access to the certificate after having obtained the public key component through other means. (CVE 2009-0085)	**2000:** 960225 **XP:** 960225 (32 bit), or 960225 (64 bit) **2003:** 960225 (32 bit), 960225 (64 bit), or 960225 Itanium **Vista:** 960225 (32 bit), or 960225 (64 bit) **2008:** 960225 (32 bit), 960225 (64 bit), or 960225 Itanium	09-007

Vulnerabilities in SChannel could allow Remote Code Execution	Fixes two vulnerabilities in the Secure Channel (SChannel) security package in Windows. The more severe of these vulnerabilities could allow remote code execution if a user visits a specially crafted Web site that is designed to exploit these vulnerabilities through an Internet Web browser. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or in an Instant Messenger message that takes users to the attacker's Web site. (CVE 2009-3555 CVE 2010-2566)	**XP:** 980436, **2003:** 980436, **Vista:** 980436, **2008:** 980436, **Windows 7:** 980436, **2008 R2:** 980436.	10-049
WordPad and Text converters remote code execution	Fixes Microsoft WordPad and Microsoft Office text converters memory corruption. (CVE 2008-4841 CVE 2009-0087 CVE 2009-0235 CVE 2009-2506)	**2000:** 973904 **XP:** 973904 **2003:** 973904	09-010 09-073
DirectX MJPEG decompression remote code execution	Corrects the way the DirectShow component of DirectX decompresses media files. (CVE 2009-0084)	**2000 (8.1):** 961373 **2000 (9.0->9.0c):** 961373 **XP:** 32-bit: 961373 64-bit: 96173 **2003:** 32-bit: 961373 64-bit: 961373 Itanium: 961373	09-011
Windows HTTP Services integer underflow	Fixes integer underflow, certificate name mismatch, and credential reflection vulnerabilities in Windows HTTP Services. (CVE 2009-0086 CVE 2009-0089 CVE 2009-0550)	**2000:** 960803 **XP:** 960803 **2003:** 960803 **Vista:** 960803 **2008:** 960803	09-013
Blended threat privilege elevation vulnerability	Fixes a privilege elevation vulnerability in Windows 2000, 2003, XP, Vista, and 2008. The vulnerability exists due to a faulty SearchPath function used for locating and opening files on windows. An attacker could exploit the vulnerability by enticing a user to download a crafted file to a specific location and then have them open an application that uses the file. (CVE 2008-2540)	**2000:** 959426 **XP:** 959426 (32 bit), or 959426 (64 bit) **2003:** 959426 (32 bit), 959426 (64 bit), or 959426 Itanium **Vista:** 959426 (32 bit), or 959426 (64 bit) **2008:** 959426 (32 bit), 959426 (64 bit), or 959426 Itanium	09-015
Microsoft SharePoint Server 2007 Remote Code Execution	Microsoft SharePoint Server 2007 has a remote code execution vulnerability. (CVE 2009-0549 CVE 2009-0557 CVE 2009-0558 CVE 2009-0559 CVE 2009-0560 CVE 2009-0561 CVE 2009-1134 CVE 2011-1989 CVE	**Microsoft SharePoint Server 2007 SP1:**KB969737 (32 bit), or KB969737 (64 bit)	09-021 11-072

	2011-1990)	**Microsoft SharePoint Server 2007 SP2:**KB2553093 (32 bit), or KB2553093 (64 bit)	
Microsoft Lync Elevation of Privilege Vulnerability (MS15-104)	An elevation of privilege vulnerability has been patched in Microsoft Lync Server 2013 and Skype for Business Server 2015. (CVE 2015-2531, CVE 2015-2532, CVE 2015-2536)	**Microsoft Lync Server 2013** :KB3080353 **Skype for Business Server 2015**:KB3080355 and KB3080352	15-104
Microsoft Lync and Skype Server Information Disclosure Vulnerability (MS15-123)	An information disclosure vulnerability has been patched in Microsoft Lync Server 2010, 2013, and Skype for Business Server 2015. (CVE 2015-6061)	**Microsoft Lync Server 2010** :KB3081089 **Microsoft Lync Server 2013** :KB3085500 **Skype for Business Server 2016**:KB2910994	15-123
Microsoft Lync and Skype Server Elevation of Privilege Vulnerability (MS15-116)	An elevation of privilege vulnerability has been patched in Microsoft Lync Server 2013 and Skype for Business Server 2015. (CVE 2015-2503)	**Microsoft Lync Server 2013** :KB3080353 **Skype for Business Server 2015**:KB2910994	15-116
Microsoft SharePoint Server 2010 Memory Corruption Vulnerability (MS15-081)	Microsoft SharePoint Server 2010 has a memory corruption vulnerability. (CVE 2015-2468)	**Microsoft SharePoint Server 2010 SP2:**KB3054960	15-081
Microsoft SharePoint Server 2010 Remote Code Execution	Microsoft SharePoint Server 2010 has a remote code execution vulnerability. (CVE 2011-1989)	**Microsoft SharePoint Server 2010 SP1:**KB2553094 (32 bit), or KB2553094 (64 bit)	11-072
Microsoft SharePoint Server 2010 & 2013 Remote Code Execution	Microsoft SharePoint Server 2010 & 2013 have a remote code execution vulnerability that can be triggered when parsing malicious documents. (CVE 2014-0260, CVE 2014-1761)	**Microsoft SharePoint Server 2010:**KB2878220 **Microsoft SharePoint Server 2013:** KB2863907	14-017 (supersedes 14-001)
Microsoft Office Web Apps 2010 Remote Code Execution	Microsoft Office Web Apps 2010 has a remote code execution vulnerability. (CVE 2011-1989)	**Microsoft Office Web Apps 2010 SP1:**KB2553095 (32 bit), or KB2553095 (64 bit)	11-072
Windows Search Contains Information Disclosure Vulnerability	Windows 2003 and XP contain an information disclosure vulnerability in Windows search due to the way file previews are generated. Exploitation	**2003 SP2:** KB963093 (32 bit), or KB963093 (64 bit)	09-023

	requires user interaction and upon a successful attack, information will be presented to the attacker. (CVE 2009-0239)	**XP SP2, SP3:** KB963093, or KB963093	
Windows kernel desktop validation vulnerabilities	Fixes four vulnerabilities by correcting the methods used in validating a change in kernel object, the input passed from user mode to the kernel and the argument passed to the system call. (CVE 2009-1123 CVE 2009-1124 CVE 2009-1125 CVE 2009-1126)	**2000:** 968537 **XP:** 968537 **2003:** 968537 **Vista:** 968537 **2008:** 968537	09-025
Windows RPC Marshalling Engine vulnerability	Fixes an elevation of privilege vulnerability by correcting the way RPC Marshalling Engine updates its internal state. (CVE 2009-0568)	**2000:** 970238 **XP:** 970238 **2003:** 970238 **Vista:** 970238 **2008:** 970238	09-026
Windows print spooler vulnerabilities	Fixes two privilege elevation vulnerabilities in the Windows print spooler, and one remote command execution vulnerability on Windows 2000. (CVE 2009-0228 CVE 2009-0229 CVE 2009-0230)	**2000:** 961501 **XP:** 961501 **2003:** 961501 **Vista:** 961501 **2008:** 961501	09-022
Microsoft DirectShow QuickTime Movie Parsing Code Execution	Fixes three vulnerabilities which could allow code execution when DirectShow parses Quicktime media files, validates pointer values and size fields. (CVE 2009-1537 CVE 2009-1538 CVE 2009-1539)	**2000:** 971633 **XP:** 971633 **2003:** 971633	09-028
Windows Embedded OpenType Font Engine vulnerabilities	Fixes a vulnerability allowing command execution when a user opens a file or web page containing Embedded OpenType fonts. (CVE 2009-0231 CVE 2009-0232)	**2000:** 961371 **XP:** 961371 **2003:** 961371 **Vista:** 961371 **2008:** 961371	09-029
Vulnerability in the OpenType Compact Font Format Driver Could Allow Elevation of Privilege	Fixes a vulnerability in the Windows OpenType Compact Font Format (CFF) driver. The vulnerability could allow elevation of privilege if a user views content rendered in a specially crafted CFF font. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users. (CVE 2010-0819 CVE 2010-2740 CVE 2010-2741)	**2000:** 980218 (Note: Windows 2000 is past its maintenance window) **XP:** 2279986 (32-bit), 2279986 (64-bit) **2003:** 2279986 (32-bit), 2279986 (64-bit), 2279986 (Itanium) **Vista:** 980218 **2008:** 980218 **Windows 7:** 980218	10-037 10-078 (supersedes 10-037 on XP and 2003)
Windows media file processing vulnerable	Fixes a vulnerability that allows remote code execution due to improper handling of specially crafted AVI format files. (CVE 2009-1545 CVE 2009-1546)	**2000:** 971557 **XP:** 971557 (32-bit), 971557 (64 bit) **2003:** 971557 (32-bit), 971557 (64 bit), 971557 (Itanium)	09-038

		Vista: 971557 (32-bit), 971557 (64-bit) **2008:** 971557 (32-bit), 971557 (64-bit), 971557 (Itanium)	
Windows Remote Desktop Connection vulnerabilities	Fixes two heap overflow vulnerabilities which could allow command execution when the client receives a specially crafted response from a RDP server or web site. (CVE 2009-1133 CVE 2009-1929)	970927	09-044
Multiple Windows ATL vulnerability	Fixes multiple vulnerabilities in Windows Active Template Library that could allow an attacker to execute arbitrary code. (CVE 2008-0015 CVE 2008-0020 CVE 2009-0901 CVE 2009-2493 CVE 2009-2494)	**Outlook:**973354 **Media Player:**973540 **ATL Component:**973507 **DHTML Component:**973869 **ActiveX:** 973525	09-037 09-055
DHTML Editing Component ActiveX Control Vulnerability	Fixes a remote code execution vulnerability in the DHTML Editing Component ActiveX Control brought on by users visiting a specially crafted web page. (CVE 2009-2519)	**2000:** 956844 **XP:** 956844 (32-bit), 956844 (64-bit) **2003:** 956844 (32-bit), 956844 (64-bit), 956844 (Itanium)	09-046
Windows Media header parsing and playback memory corruption vulnerabilities	Fixes code execution vulnerabilities in the handling of ASF format files and MP3 media files. (CVE 2009-2498 CVE 2009-2499)	**2000:** 968816 **XP SP2:** 968816 **XP SP3:** 968816 **2003:** 968816 **Vista:** 968816 **2008:** 968816	09-047
Microsoft Windows TCP/IP elevation of privilege vulnerability	Fixes several vulnerabilities in Transmission Control Protocol/Internet Protocol (TCP/IP) processing. The vulnerabilities could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of another process. If this process runs with administrator privileges, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE 2014-4076)	**2003:** 2989935	14-070
Microsoft Windows TCP/IP remote code execution vulnerability	Fixes several vulnerabilities in Transmission Control Protocol/Internet Protocol (TCP/IP) processing. The vulnerabilities could allow remote code execution if an attacker sent specially crafted TCP/IP packets over the	**2003:** 967723 **Vista:** 967723 **2008:** 967723	09-048

	network to a computer with a listening service. (CVE 2008-4609, CVE 2009-1925, CVE 2009-1926)		
Wireless LAN AutoConfig Service frame parsing remote code execution vulnerability	Fixes a remote code execution vulnerability in the Wireless LAN AutoConfig Service (wlansvc) triggered when the service receives a specially crafted wireless frame. (CVE 2009-1132)	**Vista:** 970710 (32-bit), 970710 (64-bit) **2008:** 970710 (32-bit), 970710 (64-bit)	09-049
Windows Media Player ASF file heap overflow	Fixes a vulnerability which could allow command execution when a user opens a malformed file in Windows Media Player 6.4. (CVE 2009-2527)	**2000:** 974112 **XP:** 974112 **2003:** 974112	09-052
Windows LSASS denial of service vulnerability	Fixes a vulnerability which could allow a remote attacker to crash the computer. (CVE 2009-2524)	**XP:** 975467 **2003:** 975467 **Vista:** 975467 **2008:** 975467 **7:** 975467	09-059
SMBv2 remote code execution vulnerability	Fixes a remote code execution vulnerability that could allow a remote attacker to take control of or crash the system. (CVE 2009-2526 CVE 2009-2532 CVE 2009-3103)	**Vista:** 975517 (32-bit), 975517 (64-bit) **2008:** 975517 (32-bit), 975517 (64-bit), 975517 (Itanium)	09-050
Windows WMA Voice codec vulnerability	Fixes vulnerabilities in Windows Media Runtime that could allow remote code execution (CVE 2009-0555 CVE 2009-2525)	**2000, XP and 2003 (Voice codec):** 969878 **2000 WMF 9:** 954155 **2000 WMP 9:** 975025 **2000, XP and 2003 (Decoder):** 969878 **XP SP2 WMF 9, 9.5 and 11:** 954155 **XP (Compression Manager):** 975025 **2000 WMP 9:** 975925	09-051
Windows ASN1 spoofing vulnerability	Fixes vulnerabilities in Windows CryptoAPI component when parsing ASN.1. (CVE 2009-2510 CVE 2009-2511)	**2000:** 974571 **XP:** 974571 **XP (64-bit):** 974571 **2003:** 974571 **2003 (64-bit):** 974571 **Vista:** 974571	09-056
Windows Indexing Service memory corruption vulnerability	Fixes a remote code execution vulnerability that could allow a remote attacker to execute arbitrary code with the permissions of the user loading a specially crafted web page. (CVE 2009-2507)	**2000:** 969059 **XP:** 969059 (32-bit), 969059 (64-bit) **2003:** 969059 (32-bit), 969059 (64-bit), 969059 (Itanium)	09-057

Windows kernel embedded font vulnerabilities	Fixes a remote code execution vulnerability that could allow a remote attacker to execute arbitrary code with the permissions of the user loading a specially crafted Embedded OpenType (EOT) font. (CVE 2009-1127) (CVE 2009-2513) (CVE 2009-2514)	**2000:** 969947 **XP:** 969947 (32-bit), 969947 (64-bit) **2003:** 969947 (32-bit), 969947 (64-bit), 969947 (Itanium) **Vista:** 969947 (32-bit), 969947 (64-bit) **2008:** 969947 (32-bit), 969947 (64-bit), 969947 (Itanium)	09-065
Windows WSDAPI remote code execution vulnerability	Fixes a remote code execution vulnerability that could allow a remote attacker to send specially crafted message to a computer using the Web Services on Devices API (WSDAPI) on Windows systems. The service is enabled by default on Windows Vista and Windows Server 2008. (CVE 2009-2512)	**Vista:** 973565 **2008:** 973565	09-063
Windows Internet Authentication Service vulnerabilities	Fixes vulnerabilities in the Windows PEAP and MS-CHAPv2 protocol implementations, which could lead to remote code execution in Windows 2008, privilege elevation in other server operating systems, and potential vulnerabilities in workstations. (CVE 2009-2505 CVE 2009-3677)	**2000:** 974318 **XP:** 974318 **2003:** 974318 **Vista:** 974318 **2008:** 974318	09-071
Windows LSASS IPSEC Denial-of-Service Vulnerability	Fixes a vulnerability in the Local Security Authority Subsystem Service (LSASS) which could allow a denial of service. (CVE 2009-3675)	**2000:** 974392 **2003:** 974392 (32-bit), 974392 (64-bit), 974392 (Itanium) **XP:** 974392 (32-bit), 974392 (64-bit)	09-069
Windows Embedded OpenType Font Engine Vulnerability	Fixes a remote code execution vulnerability in Windows 2000, 2003, XP, Vista, 7, and Server 2008. The vulnerability exists due to the way Windows Embedded OpenType (EOT) Font Engine decompresses specially crafted EOT fonts. (CVE 2010-0018)	**2000:** 972270 **2003:** 972270 (32-bit), 972270 (64-bit) **XP:** 972270 (32-bit), 972270 (64-bit) **Vista:** 972270 (32-bit), 972270 (64-bit) **Windows 7:** 972270 **2008:** 972270 (32-bit), 972270 (64-bit)	10-001
Microsoft Paint Integer Overflow vulnerability	Fixes a remote code execution vulnerability if a user viewed a	**2000:** 978706 **XP:** 978706	10-005

	specially crafted JPEG image file using Microsoft Paint in Windows 2000, XP and Server 2003. An attacker who successfully exploited this vulnerability could take complete control of an affected system and could then install programs; view, change, or delete data; or create new accounts. (CVE 2010-0028)	(32-bit), 978706 (64-bit) **2003:** 978706 (32-bit), 978706 (64-bit), 978706 (Itanium)	
DirectShow AVI buffer overflow	Fixes vulnerabilities in DirectShow which could allow code execution when a user opens a crafted AVI file. (CVE 2010-0250)	977914 and 975560	10-013
Windows Shell Handler vulnerability	Fixes a remote code execution vulnerability in Windows 2000, XP and Server 2003; if an application such as a Web browser passes specially crafted data to the ShellExecute API function through the Windows Shell Handler. An attacker who successfully exploited this vulnerability could take complete control of an affected system. (CVE 2010-0027)	**2000:** 975713 **XP:** 975713 (32-bit), 975713 (64-bit) **2003:** 975713 (32-bit), 975713 (64-bit), 975713 (Itanium)	10-007
Microsoft Hyper-V Server Denial of Service Vulnerability	Fixes a remote denial of service vulnerability in Windows Server 2008 Hyper-V and Windows Server 2008 R2 Hyper-V. The vulnerability could allow denial of service if a malformed sequence of machine instructions is run by an authenticated user in one of the guest virtual machines hosted by the Hyper-V server. (CVE 2010-0026)	**2008:** 977894 (64-bit) **2008 R2:** 977894 (64-bit)	10-010
Multiple vulnerabilities (MS10-012)	Fixes 4 vulnerabilities announced in Microsoft bulletin MS10-012, the most critical of which could allow remote code execution. The vulnerabilities are due to weak entropy used in encryption, bounds checking on path names, and null pointers. (CVE 2010-0020 CVE 2010-0021 CVE 2010-0022 CVE 2010-0231)	**2000 (all versions):** 971468 **XP:** 971468 **2003 (all versions):** 971468 **Vista (all versions):** 971468 **Windows 7 (all versions):** 971468 **2008 (all versions):** 971468	10-012
Multiple vulnerabilities (MS10-009)	Fixes 4 vulnerabilities announced in Microsoft bulletin MS10-009, the most critical of which could allow remote code execution. (CVE 2010-0239 CVE 2010-0240 CVE 2010-0241 CVE 2010-0242)	**Vista (all versions):** 971468 **2008 (all versions):** 971468	10-009
Multiple Data Analyzer ActiveX Control vulnerabilities	Fixes multiple vulnerabilities in Windows Data Analyzer ActiveX Control that could allow an attacker to execute arbitrary code. (CVE 2010-0252)	**ActiveX:**978262	10-008
Windows SMB Client vulnerabilities	Fixes vulnerabilities which could allow remote code execution when a user initiates an SMB connection with a malicious server. (CVE 2010-0016	**2000:** 978251 **XP:** 978251, 978251 (64-bit) **2003:** 978251,	10-006

	CVE 2010-0017)	978251 (64-bit) **Vista:** 978251, 978251 (64-bit) **Windows 7:** 978251, 978251 (64-bit) **2008:** 978251, 978251 (64-bit)	
CSRSS Local Privilege Elevation	Fixes a vulnerability in Client/Server Run-time Subsystem (CSRSS). (CVE 2010-0023)	**2000:** 978037 **XP:** 978037, 978037 (64-bit) **2003:** 978037, 978037 (64-bit)	10-011
Elevation of Privilege	Vulnerability in Windows CSRSS could Allow Elevation of Privilege. (CVE 2011-0030)	**XP:**2476687 **XP:**2476687 (64-bit) **2003:**2476687 **2003:**2476687 (64-bit)	11-010
Elevation of Privilege	Vulnerability in Windows CSRSS could Allow Elevation of Privilege. (CVE 2011-3408)	**XP:**2620712 **XP:**2620712 (64-bit) **2003:**2620712 **2003:**2620712 (64-bit) **Vista:**2620712 **Vista:**2620712 (64-bit) **2008:**2620712 **2008:**2620712 (64-bit) **Windows 7:**2620712 **Windows 7:**2620712 (64-bit) **2008 R2:**2620712 (64-bit)	11-097
Elevation of Privilege	Vulnerability in Windows CSRSS could Allow Elevation of Privilege. (CVE 2011-1281 CVE 2011-1282 CVE 2011-1283 CVE 2011-1284 CVE 2011-1870)	**XP:**2507938 **XP:**2507938 (64-bit) **2003:**2507938 **2003:**2507938 (64-bit) **Vista:**2507938 **Vista:**2507938 (64-bit) **2008:**2507938 **2008:**2507938 (64-bit) **Windows 7:**2507938 **Windows 7:**2507938 (64-bit) **2008 R2:**2507938 (64-bit)	11-056
Movie Maker and Producer Buffer Overflow vulnerability	Fixes a vulnerability which could allow remote code execution when a user opens a specially crafted Movie Maker	**XP:** 975561 (32-bit), 975561 (64-bit)	10-016

	or Microsoft Producer project file. An attacker could exploit this vulnerability to take complete control of the affected system. (CVE 2010-0265)	**Vista:** 975561 (32-bit)(MM 2.6), 975561 (32-bit)(MM 6.0), 975561 (64-bit)(MM 2.6) 975561 (64-bit)(MM 6.0) **Windows 7:** 975561 (32-bit), 975561 (64-bit)	
Vulnerability in Windows Movie Maker Could Allow Remote Code Execution	Fixes a vulnerability in Windows Movie Maker. The vulnerability could allow remote code execution if an attacker sent a specially crafted Movie Maker project file and convinced the user to open the specially crafted file. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. (CVE 2010-2564)	**XP:** 981997, **Vista:** 981997(MM 2.6), 981997(MM 6.0).	10-050
Windows Media Unicast Service transport information buffer overflow	Fixes a remote code execution vulnerability in handling transport information packets. (CVE 2010-0478)	**2000:** 980858	10-025
Windows MPEG layer 3 codec vulnerable	Fixes remote code execution vulnerability in MPEG Layer-3 codecs. (CVE 2010-0480)	**2000:** 977816, **XP:** 977816 (32-bit), 977816 (64-bit), **2003:** 977816 (32-bit), 977816 (64-bit), **Vista:** 977816 (32-bit), 977816 (64-bit), **2008:** 977816 (32-bit), 977816 (64-bit)	10-026
Windows SMB Client vulnerabilities	Fixes vulnerabilities which could allow remote code execution when a user initiates an SMB connection with a malicious server. (CVE 2009-3676 CVE 2010-0269 CVE 2010-0270 CVE 2010-0476 CVE 2010-0477)	**2000:** 980232 **XP:** 980232, 980232 (64-bit) **2003:** 980232, 980232 (64-bit), 980232 (Itanium) **Vista:** 980232, 980232 (64-bit) **2008:** 980232, 980232 (64-bit), 980232 (Itanium) **Windows 7:** 980232, 980232 (64-bit) **2008 R2:** 980232 (64-bit), 980232 (Itanium)	10-020
Windows ISATAP Component spoofing vulnerability	Fixes a spoofing vulnerability which exists in the Microsoft Windows IPv6 stack due to the way that Windows	**XP:** 978338, 978338 (64-bit) **2003:** 978338,	10-029

	checks the inner packet's IPv6 source address in a tunneled ISATAP packet. (CVE 2010-0812)	978338 (64-bit), 978338 (Itanium) **Vista:** 978338, 978338 (64-bit) **2008:** 978338, 978338 (64-bit), 978338 (Itanium)	
Windows VB script vulnerable	Fixes remote code execution vulnerability which exists due to the way VB Script interacts with help files in Internet Explorer. (CVE 2010-0483)	Apply the appropriate patch.	10-022 (superseded by MS14-011)
Windows Authenticode Verification	Fixes vulnerabilities which could allow remote code execution when a user modifies an existing signed executable file. (CVE 2010-0486 CVE 2010-0487)	**For Authenticode Signature Verification:** **2000** 978601 **XP** 978601 **XP x64** 978601 **2003** 978601 **2003 x64** 978601 **Vista** 978601 **Vista x64** 978601 **2008** 978601 **2008 x64** 978601 **Windows 7** 978601 **Windows 7 x64** 978601 **2008 R2 x64** 978601 **For Cabinet File Viewer:** **2000** 979309 **XP** 979309 **XP x64** 979309 **2003** 979309 **2003 x64** 979309 **Vista** 979309 **Vista x64** 979309 **2008** 979309 **2008 x64** 979309 **Windows 7** 979309 **Windows 7 x64** 979309 **2008 R2 x64** 979309	10-019
Windows Media Player ActiveX vulnerability	Fixes a vulnerability in Windows Media Player 9 series which could allow remote code execution. (CVE 2010-0268)	**2000** 979402 **XP SP2** 979402 **XP SP3** 979402	10-027 (superseded by 10-082 on XP SP3)
Windows kernel multiple privilege elevation vulnerabilities	Fixes multiple vulnerabilities which allow authenticated users to elevate privileges on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7. (CVE 2010-0484 CVE 2010-0485 CVE 2010-1255)	**2000 SP 4** 979559 **XP SP 2 & SP 3** 979559 **XP x64 SP 2** 979559 **2003 SP 2** 979559	10-032

		2003 x64 SP 2 979559 **2003 SP2 Itanium** 979559 **Vista SP 1 & SP 2** 979559 **Vista x64 SP 1 & SP 2** 979559 **2008 32 SP 2** 979559 **2008 x64 SP 2** 979559 **2008 Itanium SP 2** 979559 **Windows 7 32-bit** 979559 **Windows 7 x64-based** 979559 **2008 R2 x64** 979559 **2008 R2 Itanium** 979559	
Multiple ActiveX Control vulnerabilities	Fixes multiple vulnerabilities in Windows Data Analyzer ActiveX Control and Internet Explorer 8 Development Tools ActiveX Control that could allow an attacker to execute arbitrary code. (CVE 2010-0252 CVE 2010-0811)	**ActiveX:**980195	10-034
Windows Media decompression vulnerabilities	Fixes multiple vulnerabilities in DirectX, Windows Media Format and Encoder, and Asycfilt.dll allowing command execution when invalid compression data in media files is processed. (CVE 2010-1879 CVE 2010-1880)	10-033 (KB975562 superseded by MS13-011 on Windows XP and Windows Server 2003)	10-033
MS10-039 fixes `toStaticHTML` Information Disclosure Vulnerability	InfoPath 2003, 2007, and SharePoint Server 2007 have a vulnerability in the way `toStaticHTML` sanitizes HTML content in Microsoft SharePoint. (CVE 2010-1257)	**InfoPath 2003:** KB980923 **InfoPath 2007:** KB979441	10-039
Windows Help and Support Center trusted document whitelist bypass	The `MPC:HexToNum` function in `helpctr.exe` in Windows Help and Support Center on Windows XP and Windows Server 2003 does not properly handle malformed escape sequences, thereby allowing a remote attacker to bypass the trusted documents whitelist and execute arbitrary commands if a user is enticed to open a specially crafted `hcp://` URL. (CVE 2010-1885)	**XP:** KB2229593 **XP Pro x64:** KB2229593 **2003:** KB2229593 **2003 x64:** KB2229593 **2003 Itanium:** KB2229593	10-042
Canonical Display Driver vulnerable version	Windows 7 and Windows Server 2008 R2 contain an integer overflow vulnerability in the canonical display driver that could allow an attacker to cause a denial of service or take complete control of the system. (CVE	**Windows 7:**KB2032276 **2008 R2:**KB2032276	10-043

	2009-3678)		
Microsoft Windows Shell Remote Code Execution Vulnerability	A remote code execution vulnerability exists in Windows Shell, a component of Microsoft Windows. The vulnerability exists because Windows incorrectly parses shortcuts in such a way that malicious code may be executed when the icon of a specially crafted shortcut is displayed. This vulnerability is most likely to be exploited through removable drives. (CVE 2010-2568)	**XP:** 2286198 **2003:** 2286198 **Vista:** 2286198 **2008:** 2286198 **7:** 2286198 **2008 R2:** 2286198	10-046
Microsoft Windows Shell Remote Code Execution Vulnerability	A remote code execution vulnerability exists in Windows Shell, a component of Microsoft Windows. The vulnerability exists because Windows incorrectly handles files and directories with specially crafted names. Attackers can use this vulnerability to gain complete control of the system if a user is logged on with administrative user rights. (CVE 2012-0175)	**XP:** 2691442 **2003:** 2691442 **Vista:** 2691442 **2008:** 2691442 **7:** 2691442 **2008 R2:** 2691442	12-048
Over-the-network SMB packet vulnerabilities in Windows	Fixes 3 vulnerabilities announced in Microsoft bulletin MS10-054, the most critical of which could allow remote code execution. (CVE 2010-2550 CVE 2010-2551 CVE 2010-2552)	**XP:** 982214 **2003:** 982214 **Vista:** 982214 **2008:** 982214 **7:** 982214 **2008 R2:** 982214	10-054
Microsoft Windows Shell Privilege Elevation Vulnerability	A local code privilege elevation vulnerability exists in Windows Shell, a component of Microsoft Windows. The attack requires local user access and the ability to execute a specially crafted application. The vulnerability is due to improper handling of file associations performed by the ShellExecute API. (CVE 2014-1807)	**2003 SP2:** 2926765 **2003 x64 SP2:** 2926765 **Vista SP2:** 2926765 **Vista SP2 x64:** 2926765 **2008:** 2926765 **2008 x64:** 2926765 **7 SP1:** 2926765 **7 SP1 x64:** 2926765 **2008 R2:** 2926765 **8:** 2926765 **8 x64:** 2926765 **8.1:** 2926765 **8.1 x64:** 2926765 **2012** 2926765 **2012 R2** 2926765	14-027
Microsoft Tablet Input Band Use After Free Vulnerability	A remote code execution vulnerability exists when the Microsoft Tablet Input Band fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could gain user rights as the current user, including Administrative rights. An attacker could then install programs; view, change, or delete data; or create	**Vista:** 3093513 (32-bit), 3093513 (64-bit) **Windows 7:** 3093513 (32-bit), 3093513 (64-bit)	15-109

	new accounts with full user rights and permissions. (CVE 2015-2548)		
Windows cinepak codec decompression vulnerability	Fixes a vulnerability in windows cinepak codec triggered by a user opening a malformed media file. (CVE 2010-2553)	**XP:** 982665 (32-bit) 982665 (64-bit) **Vista:** 982665 (32-bit) 982665 (64-bit) **7:** 982665 (32-bit) 982665 (64-bit)	10-055
TCP/IP authenticated user privilege escalation or unauthenticated denial of service	Fixes 2 vulnerabilities announced in Microsoft bulletin MS10-058. (CVE 2010-1892 CVE 2010-1893)	**Vista:** 978886 **2008:** 978886 **7:** 978886 **2008 R2:** 978886	10-058
Windows MPEG Layer-3 Audio Decoder Buffer Overflow Vulnerability	A remote code execution vulnerability exists in the way that Microsoft DirectShow MP3 filter handles supported format files. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. (CVE 2010-1882)	**XP:** 2115168 (32-bit), 2115168 (64-bit) **2003:** 2115168 (32-bit), 2115168 (64-bit)	10-052
Windows Tracing Feature for Services	Fixes a vulnerability in the Windows Tracing Feature for Services feature which allowed for local code execution. A local user account is required. (CVE 2010-2554, CVE 2010-2555)	**Vista:** 982799 **2008:** 982799 **7:** 982799 **2008 R2:** 982799	10-059
Windows kernel vulnerable version	Fixes multiple vulnerabilities which allow authenticated users to elevate privileges on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7. (CVE 2010-0232 CVE 2010-0233 CVE 2010-0234 CVE 2010-0235 CVE 2010-0236 CVE 2010-0237 CVE 2010-0238 CVE 2010-0481 CVE 2010-0481 CVE 2010-0482 CVE 2010-0810) Fixes three vulnerabilities in the Windows kernel. A data initialization bug may be exploited when creating new threads. A double free error may be exploited during error handling. These two vulnerabilities may allow a local attacker to execute arbitrary code in kernel mode. A kernel object ACL validation routine lacks sufficient sanity checking, which may allow a local attacker to cause the system to reboot or become unresponsive. (CVE 2010-1888 CVE 2010-1889 CVE 2010-1890) Also fixes vulnerabilities which could allow elevation of privilege if an	**XP:** KB2393802 **2003:** KB2393802 **Vista:** KB2393802 **2008:** KB2393802 **Windows 7:** KB2393802	10-021 10-047 11-011

	attacker logged on locally and ran a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit these vulnerabilities. (CVE 2010-4398 CVE 2011-0045)		
Windows kernel multiple privilege elevation vulnerabilities	Fixes multiple vulnerabilities which allow authenticated users to elevate privileges on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7. (CVE 2010-1887 CVE 2010-1894 CVE 2010-1895 CVE 2010-1896 CVE 2010-1897)	**XP** 2160329 **XP x64** 2160329 **2003** 2160329 **2003 x64** 2160329 **2003 Itanium** 2160329 **Vista** 2160329 **Vista x64** 2160329 **2008** 2160329 **2008 x64** 2160329 **2008 Itanium** 2160329 **Windows 7** 2160329 **Windows 7 x64** 2160329 **2008 R2 x64** 2160329 **2008 R2 Itanium** 2160329	10-048
Microsoft Windows Service Isolation Bypass Local Privilege Escalation	Fixed a vulnerability which leverages the Windows Service Isolation feature to gain elevation of privilege. (CVE 2010-1886)	**TAPI** 982316	2264072
Microsoft Windows Insecure Library Loading vulnerability	A remote attacker could execute DLL preloading attacks through an SMB share or WebDAV.	Disable loading of libraries from WebDAV and remote network shares as described in Microsoft KB 2264107.	2269637
WordPad Word 97 Text Converter Memory Corruption Vulnerability	Fixes a vulnerability in `mswrd8.wpc` which could allow remote code execution. (CVE 2010-2563)	**XP** 2259922 **XP x64** 2259922 **2003** 2259922 **2003 x64** 2259922	10-067
Print Spooler Service remote code execution vulnerability	Fixes a remote code execution vulnerability that exists due to the way the Print Spooler Service handles data sent over RPC calls. (CVE 2010-2729)	**XP** 975558 **XP x64** 975558 **2003** 975558 **2003 x64** 975558 **Vista** 975558 **Vista x64** 975558 **2008** 975558 **2008 x64** 975558 **7** 975558 **7 x64** 975558 **2008 R2** 975558	10-061

MPEG 4 remote code execution vulnerability	Fixes a remote code execution vulnerability that exists due to the way the MPEG-4 codec handles supported format files. (CVE 2010-0818)	**XP** 975558 **XP x64** 975558 **2003** 975558 **2003 x64** 975558 **Vista** 975558 **Vista x64** 975558 **2008** 975558 **2008 x64** 975558	10-062
Active Directory LDAP LSASS privilege elevation vulnerability	Fixes a remote authenticated privilege elevation vulnerability that exists due to a heap overflow in the handling of LDAP messages in the LSASS service. (CVE 2010-0820)	**ADAM Client Patches** **XP** 982000 **2003** 982000 **2003 x64** 982000 **Active Directory Patches** **2003** 981550 **2003 x64** 981550 **2003 Itanium** 981550 **Vista** 981550 **Vista x64** 981550 **2008** 981550 **2008 x64** 981550 **7** 981550 **7 x64** 981550 **2008 R2 x64** 981550	10-068
Windows RPC Memory Corruption vulnerability	An unauthenticated remote code execution vulnerability exists in the way that the Remote Procedure Call (RPC) client implementation allocates memory when parsing specially crafted RPC responses. An attacker who successfully exploited this vulnerability could execute arbitrary code and take complete control of an affected system. (CVE 2010-2567)	**XP:** 982802 (32-bit), 982802 (64-bit) **2003:** 982802 (32-bit), 982802 (64-bit), 982802 (Itanium)	10-066
Uniscribe Font Parsing Engine Memory Corruption	Fixes a memory corruption vulnerability that exists because Windows and Office incorrectly parse specific font types. The vulnerability could allow remote code execution if a user viewed a specially crafted document or Web page with an application that supports embedded OpenType fonts. (CVE 2010-2738)	**XP:** 981322 (32-bit), 981322 (64-bit) **2003:** 981322 (32-bit), 981322 (64-bit), 981322 (Itanium) **Vista:** 981322 (32-bit), 981322 (64-bit) **2008:** 981322 (32-bit), 981322 (64-bit), 981322 (Itanium) **Office XP:** 2288608 **Office 2003:** 2288613 **2007 Office Suite:** 2288621	10-063

Uniscribe Integer Underflow Vulnerability	Fixes an integer underflow vulnerability that exists because Windows Uniscribe incorrectly parses specific font types. The vulnerability could allow remote code execution if a user viewed a specially crafted document or Web page with an application that supports embedded fonts. (CVE 2015-6130)	**Window 7:** 3108670 (32-bit), 3108670 (64-bit) **Window Server 2008 R2:** 3108670	15-130
Windows MFC Document Title Update vulnerability	Fixes a vulnerability in the Windows MFC libraries which could allow remote code execution if an attacker is able to control the title of an application written using the Microsoft Foundation Class (MFC) Library. (CVE 2010-3227)	**XP:** 2387149 (32-bit), 2387149 (64-bit) **2003:** 2387149 (32-bit), 2387149 (64-bit) **Vista:** 2387149 (32-bit), 2387149 (64-bit) **2008:** 2387149 (32-bit), 2387149 (64-bit) **7:** 2387149 (32-bit), 2387149 (64-bit) **2008 R2:** 2387149 (64-bit)	10-074
Windows Media Player Network Sharing Service vulnerability	Fixes a vulnerability in Windows Media Player Network Sharing Service which could allow remote code execution if an attacker sends a specially crafted RTSP packet to an affected system. (CVE 2010-3225)	**Vista** 2281679, 2281679 (64-bit) **Windows 7** 2281679, 2281679 (64-bit)	10-075
Embedded OpenType Font Engine vulnerability	Fixes a vulnerability in Windows which could allow remote code execution if an attacker gets a user to open a document containing a malicious embedded open-type font. (CVE 2010-1883)	**XP:** 982132 (32-bit), 982132 (64-bit) **2003:** 982132 (32-bit), 982132 (64-bit) **Vista:** 982132 (32-bit), 982132 (64-bit) **2008:** 982132 (32-bit), 982132 (64-bit) **7:** 982132 (32-bit), 982132 (64-bit) **2008 R2:** 982132 (64-bit)	10-076
Windows Common Control Library SVG vulnerability	Fixes a vulnerability in Windows which could allow remote code execution if an attacker gets a user to open a document containing a malicious Scalable Vector Graphic image using a variety of third-party image viewers or editors. (CVE 2010-2746)	**XP:** 2296011 (32-bit), 2296011 (64-bit) **2003:** 2296011 (32-bit), 2296011 (64-bit) **Vista:** 2296011 (32-bit), 2296011 (64-bit) **2008:** 2296011 (32-bit), 2296011	10-081 (superseded by 13-083 on XP Professional SP2 and Windows Server 2003).

		(64-bit) **7:** 2296011 (32-bit), 2296011 (64-bit) **2008 R2:** 2296011 (64-bit)	
Windows LPC Elevation of Privilege vulnerability	Fixes a vulnerability that could allow elevation of privilege if an attacker logs on to an affected system and runs specially crafted code that sends an LPC message to the local LRPC Server. (CVE 2010-3222)	**XP:** 2360937, 2360937 (64-bit) **2003:** 2360937, 2360937 (64-bit), 2360937 (Itanium)	10-084
Windows LPC Elevation of Privilege vulnerability	Fixes a vulnerability that could allow elevation of privilege if an attacker logs on to an affected system and runs specially crafted code that sends an LPC message to the local LRPC Server. (CVE 2013-3175)	**XP:** 2849470, 2849470 (64-bit) **2003:** 2849470, 2849470 (64-bit), 2849470 (Itanium) **Vista:** 2849470, 2849470 (64-bit) **2008:** 2849470, 2849470 (64-bit), 2849470 (Itanium) **7:** 2849470, 2849470 (64-bit) **2008 R2:** 2849470 (64-bit), 2849470 (Itanium) **8:** 2849470, 2849470 (64-bit) **2012:** 2849470 (64-bit)	13-062
Windows LPC Elevation of Privilege vulnerability	Fixes a vulnerability that could allow elevation of privilege if an attacker logs on to an affected system and runs specially crafted code that sends an LPC message to the local LRPC Server. (CVE 2013-3878)	**XP:** 2898715, 2898715 (64-bit) **2003:** 2898715, 2898715 (64-bit), 2898715 (Itanium)	13-102
Microsoft Windows JIT remote code execution vulnerability	Fixes a vulnerability in Microsoft Windows x64 .NET 4 framework that could allow arbitrary code execution. (CVE 2010-3228)	**All:** KB 2160841	10-077
Windows SChannel Denial of Service vulnerability	Fixes a vulnerability in the Secure Channel (SChannel) security package in Windows which could allow denial of service if an affected Internet Information Services (IIS) server hosting a Secure Sockets Layer (SSL)-enabled web site receives a specially crafted packet message. (CVE 2010-3229)	**Vista:** 2207566, 2207566 (64-bit) **2008:** 2207566, 2207566 (64-bit), 2207566 (Itanium) **Windows 7:** 2207566, 2207566 (64-bit) **2008 R2:** 2207566 (64-bit), 2207566 (Itanium)	10-085
Vulnerability in windows shared cluster disks	Fixes a vulnerability in windows shared cluster disks due to incorrect permission handling that could allow unauthorized users to read, write, and delete administrative shares on a failover cluster disk. (CVE 2010-3223)	**2008 R2:** 2294255 (64-bit), 2294255 (Itanium)	10-086

Elevation of Privilege Vulnerability in SharePoint Foundation 2010	Fixes multiple elevation of privilege vulnerabilities caused due to an error in the way the user input is parsed. (CVE 2013-0080, CVE 2013-0084, CVE 2013-0085)	**SharePoint Foundation 2010:** 2687418	13-024
Invalid Path Vulnerability in Microsoft Windows Defender	Fixes an invalid path vulnerability that could allow a local attacker access to administrator/SYSTEM privileges. (CVE 2013-0078)	The fix for this vulnerability is only available using windows update.	13-034
Windows NAT Driver Denial of Service Vulnerability	This security update resolves a Denial of Service Vulnerability in the Windows NAT Driver in Microsoft Windows Server 2012. The vulnerability can be triggered if an attacker sends a specially crafted ICMP packet to a target server that is running the Windows NAT Driver service. (CVE 2013-3182)	**Window Server 2012:** 2849568	13-064
MpClient Invalid Path Vulnerability in Microsoft Windows Defender	Fixes an invalid path vulnerability that could allow a local attacker access to administrator/SYSTEM privileges. (CVE 2013-3154)	**Windows 7:** 2847927 (32-bit), 2847927 (64-bit) **2008 R2:** 2847927 (64-bit)	13-058
SharePoint, Groove and Sharepoint Services multiple Vulnerabilities	This update resolves multiple Information Disclosure vulnerabilities in Microsoft SharePoint and Windows SharePoint Services. The vulnerability can be triggered if an attacker submits a specially crafted script to a target site that uses SafeHTML. (CVE 2010-3243, CVE 2010-3324)	**Microsoft Windows SharePoint Services 3.0 SP2:** 2345304 (32 Bit) or 2345304 (64 Bit) **Microsoft Office SharePoint Server 2007 SP2:** 2345212 (32 Bit) or 2345212 (64 Bit) **Microsoft SharePoint Foundation 2010:** 2345322 **Microsoft Groove Server 2010:** 2346298 **Microsoft Office Web Apps:** 2346411	10-072
Windows kernel multiple privilege elevation vulnerabilities	Fixes multiple vulnerabilities which allow authenticated users to elevate privileges on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7. (CVE 2010-2549 CVE 2010-2743 CVE 2010-2744)	**XP:** 981957 (32-bit), 981957 (64-bit) **2003:** 981957 (32-bit), 981957 (64-bit), 981957 (Itanium) **Vista:** 981957 (32-bit), 981957 (64-bit) **2008:** 981957	10-073

		(32-bit), 981957 (64-bit), 981957 (Itanium) **Win 7:** 981957 (32-bit), 981957 (64-bit) **2008 R2:** 981957 (64-bit), 981957 (Itanium)	
Windows Shell validation vulnerability	Fixes a vulnerability in a way Windows Shell validate COM object instantiation. (CVE 2010-1263)	**Vista:** 979688 (32-bit), 979688 (64-bit) **2008:** 979688 (32-bit), 979688 (64-bit), 979688 (Itanium) **Win 7:** 979688 (32-bit, 979688 (64-bit) **2008 R2:** 979688 (64-bit), 979688 (Itanium))	10-083
Windows Wordpad COM validation vulnerability	Fixes a vulnerability in a way WordPad validate COM object instantiation. (CVE 2010-1263)	**XP:** 979687 (32-bit), 979687 (64-bit) **2003:** 979687 (32-bit), 979687 (64-bit), 979687 (Itanium) **Vista:** 979687 (32-bit), 979687 (64-bit) **2008:** 979687 (32-bit), 979687 (64-bit), 979687 (Itanium) **Win 7:** 979687 (32-bit), 979687 (64-bit) **2008 R2:** 979687 (64-bit), 979687 (Itanium)	10-083
Remote code execution vulnerability in http.sys	Fixes an error in the way http.sys parses range HTTP headers. A malicious HTTP header could cause a buffer overflow on the victim machine resulting in LocalSystem code execution. Public facing IIS servers are exposed and credentials are not required for an attack. (CVE 2015-1635)	**Windows 7:** 3042553 **Windows 7 (x64):** 3042553 **Windows Server 2008 R2:** 3042553 **Windows Server 2012:** 3042553 **Windows Server 2012 R2:** 3042553 **Windows 8:** 3042553 **Windows 8(64bit):** 3042553	15-034

		Windows 8.1: 3042553 **Windows 8.1(64bit):** 3042553	
Denial of service vulnerability in http.sys	Fixes an error in the way http.sys parses some HTTP headers. A malicious HTTP header could cause a denial of service condition on the victim machine. Public facing IIS servers are exposed and credentials are not required for an attack. (CVE 2013-1305)	**Windows Server 2012:** 2829254 **Windows 8:** 2829254 **Windows 8(64bit):** 2829254	13-039
Memory Corruption Vulnerability in Windows Media Player 9.x, 10.x, 11.x	Fixes a memory corruption vulnerability in Windows Media Player (WMP). The vulnerability can be triggered if an attacker is able to entice their victim into opening specially crafted media content from a malicious web site. A successful attack would result in the attacker executing code in the context of the logged in user. (CVE 2010-2745)	**XP:** 2378111 (WMP 9, 10 or 11) **XP 64-bit:** 2378111 (WMP 10) or 2378111 (WMP 11) **2003 SP2:** 2346411 (WMP 10) **2003 SP2 64-bit:** 2346411 (WMP 10) **Vista SP1 and SP2:** 2346411 (WMP 11) **Vista SP1 and SP2 64-bit:** 2346411 (WMP 11) **2008 and SP2:** 2346411 (WMP 11) **2008 and SP2 64-bit:** 2346411 (WMP 11) **7:** 2346411 (WMP 12) **7 64-bit:** 2346411 (WMP 12) **2008 R2 64-bit:** 2346411 (WMP 12)	10-082
Forefront Unified Access Gateway Cross-Site Scripting	Fixes several cross-site scripting vulnerabilities and one redirection spoofing vulnerability in Forefront Unified Access Gateway (UAG). The vulnerability may be triggered if an attacker is able to entice their victim into clicking a specially crafted link. A successful attack would result in the attacker making requests to the UAG server in the context of the victim's logged in session. (CVE 2010-2732, CVE 2010-2733, CVE 2010-2734, CVE 2010-3936)	**UAG 2010:** KB2433585 **UAG 2010 Update 1:** KB2433584 **UAG 2010 Update 2:** KB2418933	10-089

Windows kernel NDProxy privilege elevation vulnerability	Fixes a buffer overflow vulnerability which could allow privilege elevation when a local user runs a specially crafted application. (CVE 2010-3963)	**XP:** 2440591 **2003:** 2440591	10-099
Windows kernel multiple privilege elevation vulnerabilities fixed by MS11-077	Fixes multiple vulnerabilities which could allow privilege elevation and this vulnerability could allow an attacker to run arbitrary code in kernel mode, then install programs; view, change, or delete data; or create new accounts with full administrative rights. (CVE 2011-1874, CVE 2011-1875, CVE 2011-1876, CVE 2011-1877, CVE 2011-1878, CVE 2011-1879, CVE 2011-1880, CVE 2011-1881, CVE 2011-1882, CVE 2011-1883, CVE 2011-1884, CVE 2011-1885, CVE 2011-1886, CVE 2011-1887, CVE 2011-1888, CVE 2011-1985, CVE 2011-2002, CVE 2011-2003, CVE 2011-2011)	**XP:**KB2567053 **2003:**KB2567053 **Vista:**KB2567053 **2008:**KB2567053 **Win 7:**KB2567053	11-054 11-077
Windows kernel multiple privilege elevation vulnerabilities fixed by MS10-098	Fixes multiple vulnerabilities which could allow privilege elevation when a local user runs a specially crafted application. (CVE 2010-3939, CVE 2010-3940, CVE 2010-3941, CVE 2010-3942, CVE 2010-3943, CVE 2010-3944)	**XP:** 2436673 **2003:** 2436673 **Vista:** 2436673 **2008:** 2436673 **7:** 2436673 **2008 R2:** 2436673	10-098
Windows Movie Maker insecure library loading vulnerability	Fixes a vulnerability which could allow command execution when a user loads a document from an untrusted remote location. (CVE 2010-3967)	**Vista:** 2424434	10-093
Windows Live DLL Injection Vulnerability	Fixes a local DLL injection vulnerability in the Webio.dll that is used by many Windows Live applications, as well as other Microsoft applications. This vulnerability may be exploited to allow a remote attacker to trick a user into opening a file opened by the vulnerable applications. If the file is located on a Windows file share or a WebDAV HTTP file share, the attacker can overwrite libraries that the application dynamically loads at run time with a payload of their choosing. (CVE 2010-3966)	**7:** KB2385678 **2008 R2 64-bit** KB2385678	10-095
Windows Consent UI Impersonation vulnerability	Fixes a privilege elevation vulnerability which allows an authenticated user with SeImpersonatePrivilege to execute code with LocalSystem privilege. (CVE 2010-3961)	**Vista:** 2442962 **2008:** 2442962 **7:** 2442962 **2008R2:** 2442962	10-100
Windows Task Scheduler Privilege Elevation Vulnerability	Windows Task Scheduler does not validate whether or not scheduled tasks run within the intended security context properly. An attacker could run arbitrary code with system privileges. (CVE 2010-3338)	**Vista:** 2305420 **Vista 64-bit:** 2305420 **2008:** 2305420 **2008 64-bit:** 2305420	10-092

		2008 R2: 2305420 **7:** 2305420 **7 64-bit:** 2305420	
Windows Media Encoder insecure library loading vulnerability	Fixes a vulnerability which could allow command execution when a user loads a .prx file located in the same network directory as a specially crafted DLL. (CVE 2010-3965)	**XP:** 2447961 **2003:** 2447961 **Vista:** 2447961 **2008:** 2447961	10-094
Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution	Fixes a vulnerability that could allow remote code execution if a user opens an `.ins` or `.isp` file located in the same network folder as a specially crafted library file. For an attack to be successful, a user must visit an untrusted remote file system location or WebDAV share and open a document from this location that is then loaded by a vulnerable application. (CVE 2010-3144)	**XP:** KB2443105 **2003:** KB2443105	10-097
Hyper-V Authenticated DOS Vulnerabilities	Multiple denial of service vulnerabilities exist in the Hyper-V server that can be exploited by sending a crafted packet to the VMBus. Sending such a packet requires the attacker to already be authenticated to a guest virtual machine. (CVE 2010-3960, CVE 2011-1872)	**2008 64-bit:** 2525835 **R2:** 2525835	10-102 11-047
Netlogon RPC Denial of Service	A remote authenticated denial of service vulnerability exists in implementations of the Netlogon RPC Service on affected versions of Windows Server. An attacker who successfully exploited this vulnerability could cause affected versions of the Windows Server to restart. Only Windows Servers that are configured as domain controllers and host the Netlogon service are affected by this vulnerability. (CVE 2010-2742)	**2003:** 2207559 (32-bit), 2207559 (64-bit), 2207559 (Itanium) **2008:** 2207559 (32-bit), 2207559 (64-bit) **2008 R2:** 2207559 (64-bit)	10-101
OpenType Font format driver remote code execution	Fixes three vulnerabilities which could allow remote command execution on Windows Vista, 2008, and 7, and privilege elevation on earlier operating systems. (CVE 2010-3956 CVE 2010-3957 CVE 2010-3959) Also fixes a vulnerability in the Windows OpenType Compact Font Format (CFF) driver. The vulnerability could allow remote code execution if a user views content rendered in a specially crafted CFF font. (CVE 2011-0033)	**XP:** KB2485376 **2003:** KB2485376 **Vista:** KB2485376 **2008:** KB2485376 **Windows 7:** KB2485376	10-091 11-007
Microsoft Graphics Rendering Engine Thumbnail Image Stack Buffer Overflow	Fixes a vulnerability in the Windows Graphics Rendering Engine. An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the	**XP:** 2483185 (32-bit), 2483185 (64-bit) **2003:** 2483185 (32-bit), 2483185	11-006

	logged-on user. (CVE 2010-3970)	(64-bit), 2483185 (Itanium) **Vista:** 2483185 (32-bit), 2483185 (64-bit) **2008:** 2483185 (32-bit), 2483185 (64-bit), 2483185 (Itanium)	
Backup Manager Insecure Library Loading Vulnerability	Fixes a remote code execution vulnerability in the Microsoft Windows Backup Manager. An attacker who successfully exploited this vulnerability could take complete control of an affected system and could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE 2010-3145)	**Vista:** 2478935 (32 bit), 2478935 (64 bit)	11-001
Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	Fixes vulnerabilities which could allow elevation of privilege if an attacker logged on locally and ran a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit these vulnerabilities. (CVE 2011-0662 CVE 2011-0665 CVE 2011-0666 CVE 2011-0667 CVE 2011-0670 CVE 2011-0671 CVE 2011-0672 CVE 2011-0673 CVE 2011-0674 CVE 2011-0675 CVE 2011-0676 CVE 2011-0677 CVE 2011-1225 CVE 2011-1226 CVE 2011-1227 CVE 2011-1228 CVE 2011-1229 CVE 2011-1230 CVE 2011-1231 CVE 2011-1232 CVE 2011-1233 CVE 2011-1234 CVE 2011-1235 CVE 2011-1236 CVE 2011-1237 CVE 2011-1238 CVE 2011-1239 CVE 2011-1240 CVE 2011-1241 CVE 2011-1242) Also fixes five vulnerabilities which could allow elevation of privileges if an attacker logged on locally and was able to execute a specially crafted program. (CVE 2011-0086 CVE 2011-0087 CVE 2011-0088 CVE 2011-0089 CVE 2011-0090)	**XP:** KB2506223 **2003:** KB2506223 **Vista:** KB2506223 **2008:** KB2506223 **Windows 7:** KB2506223	11-034 11-012
Windows SMB Server Transaction Vulnerability	Fixes multiple vulnerabilities in SMB server and SMB client which could allow remote code execution. (CVE 2011-0661)	**XP:** 2508429 (32-bit), 2508429 (64-bit) **2003:** 2508429 (32-bit), 2508429 (64-bit), **Vista:** 2508429 (32-bit), 2508429 (64-bit), **2008:** 2508429 (32-bit), 2508429	11-020

		(64-bit), **Windows 7:** 2508429 (32-bit), 2508429 (64-bit), **Windows 7 SP1:** 2508429 (32-bit), 2508429 (64-bit), **2008 R2:** 2508429 (64-bit), **2008 R2 SP1:** 2508429 (64-bit)	
Microsoft Data Access Component remote code execution (MS11-002)	Fixes two vulnerabilities which could allow remote execution in the way it validates third-party API usage and memory allocation. (CVE 2011-0026 CVE 2011-0027)	**XP:** 2419632 (32-bit), 2419632 (64-bit) **2003:** 2419635 (32-bit), 2419635 (64-bit), **Vista:** 2419640 (32-bit), 2419640 (64-bit), **2008:** 2419640 (32-bit), 2419640 (64-bit), **Windows 7:** 2419640 (32-bit), 2419640 (64-bit), **2008 R2:** 2419640 (64-bit)	11-002
Windows DNS Resolution Vulnerability	Fixes a vulnerability in the DNS client which could allow remote code execution if an attacker is able to deliver specially crafted LLMNR broadcast packets to the target system. (CVE 2011-0657)	**XP:** 2509553 (32-bit), 2509553 (64-bit) **2003:** 2509553 (32-bit), 2509553 (64-bit), **Vista:** 2509553 (32-bit), 2509553 (64-bit), **2008:** 2509553 (32-bit), 2509553 (64-bit), **Windows 7:** 2509553 (32-bit), 2509553 (64-bit), **2008 R2 SP1:** 2509553 (64-bit)	11-030
Windows Active Directory SPN validation denial of service	Fixes a vulnerability which could allow an administrator on a computer in the domain to downgrade the target from Kerberos to NTLM, possibly leading to a denial of service. (CVE 2011-0040)	**2003:** 2478953	11-005
Windows LSASS length validation vulnerability	Fixes a privilege elevation vulnerability which could allow an authenticated user to take complete control of the system. (CVE 2011-0039)	**XP:** 2478960 **2003:** 2478960	11-014
Vulnerabilities in DirectShow and Windows Media Player	Fixes remote code execution vulnerabilities in DirectShow and Windows Media Player. (CVE 2011-0032 CVE 2011-0042)	**XP:** 2502898 (Windows XP Media Center Edition 2005),	11-015

		2479943 (32-bit), 2479943 (Pro 64-bit) **Vista:** 2479943 (32-bit), 2479943 (64-bit) **Win 7:** 2479943 (32-bit), 2479943 (64-bit) **2008 R2:** 2479943 (64-bit)	
Vulnerabilities in Windows Media Center TV Pack	Fixes remote code execution vulnerabilities in Windows Media Center TV Pack. (CVE 2011-0032 CVE 2011-0042)	**Vista:** 2494132 (32-bit), 2494132 (64-bit)	11-015
JScript and VBScript information disclosure vulnerability	Fixes an information disclosure vulnerability due to a memory corruption error. (CVE 2011-0031)	**Win 7:** 2475792 (32-bit) 2475792 (64-bit) **2008 R2:** 2475792	11-009
VBScript Memory Corruption Vulnerability	Fixes a remote code execution vulnerability due to the way the VBScript engine handles objects in memory. (CVE 2014-0271)	Apply the appropriate patch or patches referenced in Microsoft Security Bulletin MS14-011.	14-011
VBScript Memory Corruption Vulnerability	Fixes a remote code execution vulnerability due to the way the VBScript engine, when rendered in Internet Explorer, handles objects in memory. (CVE 2014-6363)	Apply the appropriate patch or patches referenced in Microsoft Security Bulletin MS14-084.	14-084
Windows Remote Desktop Insecure Library Loading Vulnerability	Fixes a vulnerability which could allow remote code execution if a user opens a legitimate Remote Desktop configuration (`.rdp`) file located in the same network folder as a specially crafted library file. (CVE 2011-0029)	**XP:** 2483618 (32-bit 5.2), 2481109 (32-bit 6.1), 2481109 (64-bit 6.0), 2483614 (32-bit 7.0) **2003:** 2481109 (32-bit) 6.0, 2481109 (64-bit) 6.0 **Vista:** 2481109 (32-bit) 6.1, 2481109 (64-bit) 6.1, 2483614 (32-bit) 7.0, 2483614 (64-bit) 7.0 **2008:** 2481109 (32-bit) 6.1, 2481109 (64-bit) 6.1 **Win 7:** 2483614 (32-bit) 7.0, 2483614 (64-bit) 7.0	11-017

		2008 R2: 2483614 (64-bit) 7.0	
Windows MHTML Script Injection Vulnerability	Fixes a vulnerability which could allow an attacker to run MIME-formated MHTML requests in the wrong security context. This may result in an information disclosure, similar to a cross-site scripting attack. (CVE 2011-0096)	**XP:**2503658 (32-bit), 2503658 (64-bit) **2003:**2503658 (32-bit), 2503658 (64-bit) **Vista:**2503658 (32-bit), 2503658 (64-bit) **2008:**2503658 (32-bit), 2503658 (64-bit) **Win 7:**2503658 (32-bit), 2503658 (64-bit) **2008 R2:**2503658 (64-bit)	11-026
Multiple ActiveX Control vulnerabilities	Fixes multiple vulnerabilities in WMITools ActiveX Control, Internet Explorer 8 Development Tools ActiveX Control, and Windows Messenger ActiveX Control that could allow an attacker to execute arbitrary code. (CVE 2010-0811 CVE 2010-3973 CVE 2011-1243)	**ActiveX:**KB2508272	11-027
Windows Fax Cover Page Remote Code Execution Vulnerability (MS11-024)	Fixes a vulnerability in Windows Fax Cover Page Editor which improperly parses malformed cover pages. Successful exploitation could give the attacker the same privileges as the logged on user. (CVE 2010-3974 CVE 2010-4701)	**XP 32-bit:**2491683 and 2506212 **XP 64-bit:**2491683 and 2506212 **2003 32-bit:**2491683 and 2506212 **2003 64-bit:**2491683 and 2506212 **Vista 32-bit:**2491683 and 2506212 **Vista 64-bit:**2491683 and 2506212 **2008 32-bit:**2491683 and 2506212 **2008 64-bit:**2491683 and 2506212 **Windows 7 32-bit:**2491683 and 2506212 **Windows 7 64-bit:**2491683 and 2506212	11-024

		2008 R2:2491683 and 2506212	
Windows GDI+ Integer Overflow	Fixes a vulnerability which could allow remote code execution if the user opens a specially crafted Windows Enhanced Metafile (EMF) image file. (CVE 2011-0041)	**XP:** 2412687, 2412687 (64-bit) **2003:** 2412687, 2412687 (64-bit) **Vista:** 2412687, 2412687 (64-bit) **2008:** 2412687, 2412687 (64-bit)	11-029
Windows SMB Client vulnerabilities	Fixes vulnerabilities which could allow remote code execution if an attacker sent a specially crafted SMB response to a client-initiated SMB request. To exploit these vulnerabilities, an attacker must convince the user to initiate an SMB connection to a specially crafted SMB server. (CVE 2011-0654 CVE 2011-0660)	**XP:** 2511455, 2511455 (64-bit) **2003:** 2511455, 2511455 (64-bit) **Vista:** 2511455, 2511455 (64-bit) **2008:** 2511455, 2511455 (64-bit) **Windows 7:** 2511455, 2511455 (64-bit) **2008 R2:** 2511455 (64-bit)	11-019
WordPad Text Converter Vulnerability	Fixes a vulnerability which could allow remote code execution if a user opens a specially crafted Word file that includes a malformed structure. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE 2011-0028)	**XP** 2485663, 2485663 (64-bit) **2003** 2485663, 2485663 (64-bit)	11-033
Windows OpenType CFF vulnerability	Fixes a vulnerability which could allow remote code execution in the way that the OpenType Font (OTF) driver improperly parses specially crafted OpenType fonts. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE 2011-0034)	**XP** 2507618, 2507618 (64-bit) **2003** 2507618, 2507618 (64-bit) **Vista:** 2507618, 2507618 (64-bit) **2008:** 2507618, 2507618 (64-bit) **Windows 7:** 2507618, 2507618 (64-bit) **2008 R2:** 2507618 (64-bit)	11-032
Ancillary Function Driver	Fixes a vulnerability in the Microsoft Windows Ancillary Function Driver (AFD). A local user with valid login credentials could exploit this vulnerability to elevate privileges by executing a specially crafted application. (CVE 2011-1249)	**XP** 2503665, 2503665 (64-bit) **2003** 2503665, 2503665 (64-bit) **Vista** 2503665, 2503665 (64-bit) **2008** 2503665, 2503665 (64-bit) **Windows 7:** 2503665, 2503665 (64-bit) **2008 R2:** 2503665 (64-bit)	11-046, superseded by MS14-040 for Windows Vista (32-bit) Service Pack 2 and Windows Server 2008 (32-bit) Service Pack 2.

Ancillary Function Driver	Fixes a vulnerability in the Microsoft Windows Ancillary Function Driver (AFD). A local user with valid login credentials could exploit this vulnerability to elevate privileges by executing a specially crafted application. (CVE 2011-2005)	**XP** 2592799, 2592799 (64-bit) **2003** 2592799, 2592799 (64-bit)	11-080
Ancillary Function Driver	Fixes a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if an attacker logs on to a user's system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit the vulnerabilities. (CVE 2013-3887)	**XP x64 Edition:**KB2875783 **2003 x64 Edition:**KB2875783 **Vista x64 Edition:**KB2875783 **2008:**KB2875783 **Windows 7:**KB2875783 **2008 R2:**KB2875783 **Windows 8:**KB2875783 **2012:**KB2875783	13-093, superseded by MS14-040 on all supported 64-bit platforms (i.e., not XP).
WinVerifyTrust vulnerability	Fixes a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user or application runs or installs a specially crafted, signed portable executable (PE) file on an affected system. (CVE 2013-3900)	**XP:**KB2893294 **XP x64:**KB2893294 **2003:**KB2893294 **2003 x64:**KB2893294 **Vista:**KB2893294 **Vista x64:**KB2893294 **2008:**KB2893294 **2008 x64:**KB2893294 **Windows 7:**KB2893294 **Windows 7 x64:**KB2893294 **2008 R2:**KB2893294 **Windows 8:**KB2893294 **Windows 8 x64:**KB2893294 **Windows 8.1:**KB2893294 **Windows 8.1 x64:**KB2893294 **2012:**KB2893294 **2012 R2:**KB2893294	13-098
Ancillary Function Driver	Fixes two vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to a user's system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit the vulnerabilities.	**XP x64 Edition:**KB2645640 **2003:**KB2645640 **2003 x64 Edition:**KB2645640 **Vista x64 Edition:**KB2645640 **2008:**KB2645640	12-009, superseded by MS14-040 for Windows Server 2003 (32-bit) Service Pack 2.

	(CVE 2012-0148 CVE 2012-0149)	**Windows 7:**KB2645640 **2008 R2:**KB2645640	
Windows SMB Server vulnerability	Fixes a vulnerability which could allow remote denial of service attacks from an unauthenticated user. (CVE 2011-1267)	**Vista** 2536275, 2536275 (64-bit) **2008** 2536275, 2536275 (64-bit) **Windows 7:** 2536275, 2536275 (64-bit) **2008 R2:** 2536275 (64-bit)	11-048
Windows Distributed File System vulnerabilities	Fixes a vulnerability which could allow remote denial of service and remote code execution attacks from an unauthenticated user. (CVE 2011-1868 CVE 2011-1869)	**XP:** (32-bit), (64-bit) **2003:** (32-bit), (64-bit) **Vista:** (32-bit), (64-bit) **2008:** (32-bit), (64-bit) **Windows 7:** (32-bit), (64-bit) **2008 R2:** (64-bit)	11-042
Active Directory Certificate Services Web Enrollment Vulnerability	A reflective cross-site scripting vulnerability may allow an attacker to execute scripts under the context of a user's Internet Explorer client. This may allow an attacker to steal session data or perform a phishing attack. (CVE 2011-1264)	**2003:** 2518295 **2008:** 2518295 **2008 R2:** 2518295	11-051
Windows Kernel-Mode drivers remote code execution vulnerability	Fixes a vulnerability which could allow remote code execution attacks by enticing a user to visit a specially crafted web page. (CVE 2011-1873)	**XP:** (64-bit), **2003:** (64-bit), **Vista:** (64-bit), **2008:** (64-bit), **Windows 7:** (64-bit), **2008 R2:** (64-bit)	11-041
Forefront Threat Management Gateway Vulnerability	Fixes a vulnerability which could allow remote code execution if an attacker leveraged a client computer to make specific requests on a system where the Threat Management Gateway (TMG) firewall client is used. (CVE 2011-1889)	**Forefront TMG:** KB2520426	11-040
Microsoft Forefront Protection for Exchange Vulnerability	Fixes a vulnerability which could allow remote code execution if a specially crafted email message is scanned. (CVE 2014-0294)	**Forefront Protection:** KB2927022	14-008
Windows SMB Client vulnerabilities	Fixes vulnerabilities which could allow remote code execution if an attacker sent a specially crafted SMB response to a client-initiated SMB request. To exploit these vulnerabilities, an attacker must convince the user to initiate an SMB connection to a specially crafted SMB server. (CVE 2011-1268)	**XP:** 2536276, 2536276 (64-bit) **2003:** 2536276, 2536276 (64-bit) 2536276 (Itanium) **Vista:** 2536276, 2536276 (64-bit) **2008:** 2536276, 2536276 (64-bit)	11-043

		2536276 (Itanium) **Windows 7:** 2536276, 2536276 (64-bit) **2008 R2:** 2536276 (64-bit) **2008 R2:** 2536276 (Itanium)	
MHTML Mime-formatted information disclosure (MS11-037)	Fixes an information disclosure vulnerability in the way that MHTML protocol handler interprets MIME-formatted requests. (CVE 2011-1894)	**XP** 2544893, 2544893 (64-bit) **2003** 2544893, 2544893 (64-bit) **Vista** 2544893, 2544893 (64-bit) **2008** 2544893, 2544893 (64-bit) **Windows 7** 2544893, 2544893 (64-bit) **2008 R2** 2544893 (64-bit)	11-037
Windows OLE Automation Underflow vulnerability (MS11-038)	Fixes a remote code execution vulnerability in OLE Automation. (CVE 2011-0658)	**XP** 2476490, 2476490 (64-bit) **2003** 2476490, 2476490 (64-bit) **Vista** 2476490, 2476490 (64-bit) **2008** 2476490, 2476490 (64-bit) **Windows 7** 2476490, 2476490 (64-bit) **2008 R2** 2476490 (64-bit)	11-038
Windows CSRSS Privilege Escalation Vulnerability	Fixes a local privilege escalation vulnerability in the Windows Client /Server Run-time Subsystem (CSRSS). Authenticated users may be able to execute code under the context of other users. (CVE 2011-1967)	**XP** 2567680, 2567680 (64-bit) **2003** 2567680, 2567680 (64-bit) **Vista** 2567680, 2567680 (64-bit) **2008** 2567680, 2567680 (64-bit) **Windows 7** 2567680, 2567680 (64-bit) **2008 R2** 2567680 (64-bit)	11-063
Elevation of Privilege Vulnerabilities in Windows (MS11-062)	Fixes a vulnerability in Remote Access Service NDISTAPI driver. (CVE 2011-1974)	**XP** 2566454, 2566454 (64-bit) **2003** 2566454, 2566454 (64-bit)	11-062
Microsoft Remote Desktop Protocol Denial of Service Vulnerability (MS11-065)	If the Remote Desktop Protocol is enabled but not patched, a maliciously-crafted sequence of RDP packets sent by a remote, unauthenticated attacker could cause a denial of service and possibly restart the target system. (CVE 2011-1968)	**XP 32-bit SP3** 2570222 **XP 64-bit SP2** 2570222 **2003 32-bit SP2** 2570222 **2003 64-bit SP2**	11-065

		2570222 **2003 Itanium SP2** 2570222	
Microsoft Active Accessibility Insecure Library Loading Vulnerability	A remote code execution vulnerability exists in the way that the Microsoft Active Accessibility component handles the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. (CVE 2011-1247)	**XP:** 2564958 (32-bit), 2564958 (64-bit) **2003:** 2564958 (32-bit), 2564958 (64-bit) **Vista:** 2564958 (32-bit), 2564958 (64-bit) **2008:** 2564958 (32-bit), 2564958 (64-bit) **Win 7:** 2564958 (32-bit), 2564958 (64-bit) **2008 R2:** 2564958 (64-bit)	11-075
Windows Media Center Remote Code Execution Vulnerability	A remote code execution vulnerability exists in the way that Windows Media Center handles the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. (CVE 2011-2009)	**Vista:** 2579692 (32-bit), 2579692 (64-bit)	11-076
Microsoft Data Access Component Insecure Library Loading Vulnerability	A remote code execution vulnerability exists in the way that the Windows Data Access Tracing component handles the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. (CVE 2011-1975)	**Windows 7:** 2560656 (32-bit), 2560656 (64-bit) **2008 R2:** 2560656 (64-bit)	11-059
Windows Kernel Metadata Parsing DOS Vulnerability	A denial of service vulnerability exists in Windows due to the way the kernel parses file meta-data when browsing to a folder. An attacker who successfully exploited this vulnerability could cause the affected system to crash. (CVE 2011-1971)	**Vista:** 2556532 (32-bit), 2556532 (64-bit) **2008:** 2556532 (32-bit), 2556532 (64-bit) **Windows 7:** 2556532 (32-bit), 2556532 (64-bit) **2008 R2:** 2556532 (64-bit)	11-068 (superseded by 11-098 on 32-bit versions of Windows Vista, Windows Server 2008, and Windows 7)
Windows Kernel Exception Handler Vulnerability	A privilege elevation vulnerability exists in Windows due to the kernel's failure to initialize some objects in memory. An attacker would have to log on	**XP:** 2633171 (32-bit) **2003:** 2633171 (32-bit)	11-098

	locally to an affected system and run a specially crafted application designed to exploit the vulnerability. The vulnerability could not be exploited remotely or by anonymous users. (CVE 2011-2018)	**Vista:** 2633171 (32-bit) **2008:** 2633171 (32-bit) **Windows 7:** 2633171 (32-bit)	
Windows IME Library Injection Vulnerability	An insecure library loading vulnerability exists in several Windows components. An attacker may exploit this vulnerability by placing a malicious library file (DLL) in the same folder as documents with the following extensions: .txt, .rft, .doc. (CVE 2011-1991)	**XP:** 2570947 (32-bit), 2570947 (64-bit) **2003:** 2570947 (32-bit), 2570947 (64-bit) **Vista:** 2570947 (32-bit), 2570947 (64-bit) **2008:** 2570947 (32-bit), 2570947 (64-bit) **Windows 7:** 2570947 (32-bit), 2570947 (64-bit) **2008 R2:** 2570947 (64-bit)	11-071
Forefront Unified Access Gateway Cross-Site Scripting and Java Applet	Fixes several cross-site scripting vulnerabilities and one client browser JAVA applet vulnerability in Forefront Unified Access Gateway (UAG). The XSS vulnerabilities may be triggered if an attacker is able to entice their victim into clicking a specially crafted link. A successful attack would result in the attacker making requests to the UAG server in the context of the victim's logged in session. The JAVA applet vulnerability may allow an attacker to compromise an end-user's work station if they can convince the user view a page containing malicious content. (CVE 2011-1895, CVE 2011-1896, CVE 2011-1897, CVE 2011-1969, CVE 2011-2012)	**UAG 2010:** 2522482, 2522483 (Update1), 2522484 (Update2), 2522485 (SP1)	11-079
Windows Active Directory LDAPS Authentication Bypass	Fixes a vulnerability in Windows Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS) that could allow privilege elevation if (a) Active Directory is configured to use LDAP over SSL (LDAPS) and (b) an attacker acquires a revoked certificate that is associated with a valid domain account and then uses that revoked certificate to authenticate to the Active Directory domain. By default, Active Directory is not configured to use LDAP over SSL. (CVE 2011-2014)	**XP:** ADAM: 2616310, 2616310 (64-bit) **2003:** AD: 2601626, 2601626 (64-bit); ADAM: 2616310, 2616310 (64-bit) **Vista:** AD LDS: 2601626, 2601626 (64-bit) **2008:** AD & AD LDS: 2601626, 2601626 (64-bit) **7:** AD LDS: 2601626, 2601626 (64-bit)	11-086

		2008 R2: AD & AD LDS: 2601626	
Vulnerability in Windows Kernel-Mode Drivers Could cause a Denial of Service	Fixes a vulnerability in Windows Kernel-Mode Drivers that could cause a denial of service when opening specially crafted true types fonts. (CVE 2011-2004)	KB2617657 **Win 7:** 32-bit, 64-bit **2008 R2:** 64-bit, Itanium	11-084
Windows TCP/IP Elevation of Privilege and Firewall Bypass Vulnerabilities (MS12-032)	Fixes two vulnerabilities in Microsoft Windows. The more severe of these vulnerabilities could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application. (CVE 2012-0174 CVE 2012-0179) Also fixes two denial of service vulnerabilities in windows TCP/IP stack. (CVE 2011-1871 CVE 2011-1965) Also fixes a remote code execution vulnerability in Windows TCP/IP stack. (CVE 2011-2013)	**Vista:**KB2688338 **Vista x64:** KB2688338 **2008:**KB2688338 **2008 x64:**KB2688338 **Windows 7:**KB2688338 **Windows 7 x64:** KB2688338 **2008 R2 x64:** KB2688338	11-064 11-083 12-032
Microsoft Windows Mail Insecure Library Loading Vulnerability	A vulnerability in Microsoft Windows Mail and Windows Meeting Space could permit remote code execution using a malicious DLL library. (CVE 2011-2016)	KB2620704 **Vista SP2:** 32-bit, 64-bit **2008 SP2:** 32-bit, 64-bit, Itanium **Windows 7 & SP1:** 32-bit, 64-bit **2008 R2 & SP1:** 64-bit, Itanium	11-085
Multiple ActiveX Control vulnerabilities	Fixes multiple vulnerabilities in the Microsoft Time ActiveX Control that could allow an attacker to gain the same privileges as the logged on user. (CVE 2011-3397)	KB2618451 **XP:** 32-bit, 64-bit **2003:** 32-bit, 64-bit, Itanium **Vista:** 32-bit, 64-bit **2008:** 32-bit, 64-bit, Itanium **Win 7:** 32-bit, 64-bit **2008 R2:** 64-bit, Itanium	11-090
Windows TrueType font parsing vulnerability	Fixes a vulnerability in Windows Kernel-Mode Drivers that could allow privilege elevation and this vulnerability could allow an attacker to run arbitrary code in kernel mode, then install programs; view, change, or delete data; or create new accounts with full administrative rights. (CVE 2011-3402)	KB2639417 **XP:** 32-bit, 64-bit **2003:** 32-bit, 64-bit **Vista:** 32-bit, 64-bit **2008:** 32-bit, 64-bit **Win 7:** 32-bit, 64-bit **2008 R2:** 64-bit	11-087
Active Directory and ADAM denial of service	Fixes a vulnerability which could allow an attacker who has credentials to an Active Directory domain to cause a denial of service. (CVE 2013-1282)	**XP:** 2801109 **2003:** 2772930 (Active Directory) **2003:** 2801109 (ADAM) **Vista:** 2772930 **2008:** 2772930 **7:** 2772930 **2008 R2:**	13-032

		2772930 **8:** 2772930 **2012:** 2772930	
Active Directory and ADAM buffer overflow	Fixes a privilege elevation vulnerability which could allow command execution by an attacker who has credentials to an Active Directory domain. (CVE 2011-3406)	**XP:** 2626416 **2003:** 2621146 (Active Directory) **2003:** 2626416 (ADAM) **Vista:** 2621146 **2008:** 2621146 **7:** 2621146 **2008 R2:** 2621146	11-095
Windows Media Player DVR-MS File Parsing Vulnerability	Fixes an error in the DirectShow library of Windows Media Center and Media Player where DVR-MS files (with the *dvr-ms* extension) are improperly parsed. An attacker could leverage this bug to corrupt memory and gain control of execution over the target system. (CVE 2011-3401)	**XP** 2619339 **Vista** 2619339 **7** 2619339	11-092
Object Linking and Embedding (OLE) Vulnerability	Fixes an error in the handling of OLE objects in compound documents. An attacker could leverage this bug to corrupt memory and gain control of execution over the target system. (CVE 2011-3400)	**XP** 2624667 **2003** 2624667	11-093
Windows Kernel Security Feature Bypass Vulnerability	Fixes a vulnerability in Microsoft Windows. The vulnerability could allow an attacker to bypass the SafeSEH security feature in a software application. An attacker could then use other vulnerabilities to leverage the structured exception handler to run arbitrary code. (CVE 2012-0001)	**2003:**KB2644615 **Vista:**KB2644615 **2008:**KB2644615 **Win 7:**KB2644615	12-001
Microsoft Office ClickOnce Vulnerability	A remote code execution vulnerability exists in the Microsoft Office ClickOnce embedded application feature due to the way Windows validates package contents. (CVE 2012-0013)	**XP:** 2584146 (32-bit), 2584146 (64-bit) **2003:** 2584146 (32-bit), 2584146 (64-bit) **Vista:** 2584146 (32-bit), 2584146 (64-bit) **2008:** 2584146 (32-bit), 2584146 (64-bit) **Windows 7:** 2584146 (32-bit), 2584146 (64-bit) **2008 R2:** 2584146 (64-bit)	12-005
Windows CSRSS Privilege Escalation Vulnerability	Fixes a local privilege escalation vulnerability in the Windows Client /Server Run-time Subsystem (CSRSS). Authenticated users may be able to execute code under the context of other users. (CVE 2012-0005)	**XP** 2646524 **2003** 2646524 **Vista** 2646524 **2008** 2646524	12-003

Windows CSRSS Privilege Escalation Vulnerability	Fixes a local privilege escalation vulnerability in the Windows Client /Server Run-time Subsystem (CSRSS). Authenticated users may be able to execute code under the context of other users. (CVE 2013-1295)	**XP** 2820917 **2003** 2820917 **Vista** 2820917 **2008** 2820917	13-033
Windows Object Packager Insecure Executable Launching Vulnerability	Fixes a vulnerability in the way that Windows registers and uses the Windows Object Packager that could allow remote code execution if a user opens a legitimate file with an embedded packaged object that is located in the same network directory as a specially crafted executable file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. (CVE 2012-0009)	**XP:** KB2598479 (32-bit), 2603381 (64-bit) **2003:** 2603381 (32-bit), 2603381 (64-bit)	12-002
Windows Multimedia Library MIDI Vulnerability	Fixes a vulnerability in the way that Windows Multimedia Library parses MIDI files. Windows Multimedia Library is used by applications such as Windows Media Player to work with audio and video. An attacker who convinces a user to open a specially crafted MIDI file could run arbitrary code in the context of the current user. (CVE 2012-0003)	**XP:** 2628259 (Windows XP Media Center Edition 2005), 2598479 (32-bit), 2598479 (64-bit) **2003:** 2598479 (32-bit), 2598479 (64-bit) **Vista:** 2598479 (32-bit), 2598479 (64-bit) **2008:** 2598479 (32-bit), 2598479 (64-bit)	12-004
Windows DirectShow media file parsing vulnerability	Fixes a vulnerability in the way that Windows DirectShow (a component of Windows DirectX) handles media files. An attacker who convinces a user to open a specially crafted media file could run arbitrary code in the context of the current user. (CVE 2012-0004)	**XP:** 2631813 (32-bit), 2631813 (64-bit) **2003:** 2631813 (32-bit), 2631813 (64-bit) **Vista:** 2631813 (32-bit), 2631813 (64-bit), 2628642 (32-bit), 2628642 (64-bit) **2008:** 263183 (32-bit), 2603381 (64-bit) **7:** 263183 (32-bit), 263183 (64-bit) **2008R2:** 263183	12-004
SSL and TLS Protocols Vulnerable Implementation	A vulnerability exists within the SSL 3.0 and TLS 1.0 protocols through which an attacker who has access to an active (encrypted) SSL connection — a “man-in-the-middle” attack — may be able to break the encryption and read the content being transmitted. No actual exploit was known until 2011,	**XP 32-bit SP3** 2585542 **XP 64-bit SP2** 2585542, 2638806 **2003 32-bit SP2** 2585542, 2638806 **2003 64-bit SP2** 2585542, 2638806	12-006

	when an exploit tool named “BEAST” demonstrated a block-wise chosen-plaintext attack using vulnerable Web browsers and a crafted Web site. SSL 3.0 and TLS 1.0, using CBC mode, are vulnerable. TLS 1.1 and 1.2, and all encryption methods which do not use CBC mode, are unaffected by this vulnerability. (CVE 2011-3389)	**2003 Itanium SP2** 2585542, 2638806 **Vista 32-bit SP2** 2585542 **Vista 64-bit SP2** 2585542 **2008 32-bit SP2** 2585542 **2008 64-bit SP2** 2585542 **2008 Itanium SP2** 2585542 **W7 32-bit to SP1** 2585542 **W7 64-bit to SP1** 2585542 **2008 R2 64-bit to SP1** 2585542 **2008 R2 Itanium to SP1** 2585542 Additional Fix Information	
MS Windows Kernel-Mode Drivers Remote Code Execution Vulnerability	Two vulnerabilities exist in kernel-mode drivers which, if exploited, could give an attacker the ability to execute arbitrary program code on the vulnerable computer. (CVE 2011-5046, CVE 2012-0154)	KB2660465 **XP:** 32-bit, 64-bit **2003:** 32-bit, 64-bit, Itanium **Vista:** 32-bit, 64-bit **2008:** 32-bit, 64-bit, Itanium **Win 7:** 32-bit, 64-bit **2008 R2:** 64-bit, Itanium	12-008
Windows Kernel-Mode Drivers Elevation of Privilege vulnerabilities	Three privately reported vulnerabilities in Microsoft Windows kernel-mode drivers could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. (CVE 2013-1285 CVE 2013-1286 CVE 2013-1287)	**XP 32-bit:**KB2807986 **XP 64-bit:**KB2807986 **2003 32-bit:**KB2807986 **2003 64-bit:**KB2807986 **Vista 32-bit:**KB2807986 **Vista 64-bit:**KB2807986 **2008 32-bit:**KB2807986 **2008 64-bit:**KB2807986 **W7 32-bit:**KB2807986 **W7 64-bit:**KB2807986 **2008 R2:**KB2807986 **W8 32-bit:**KB2807986	13-027

		W8 **64-bit:**KB2807986 **2012:**KB2807986	
MS Windows Kernel-Mode Drivers Elevation of Privilege vulnerabilities	One publicly disclosed and one privately reported vulnerability exist in Microsoft Windows kernel-mode drivers which could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. (CVE 2012-1890 CVE 2012-1893) The vulnerabilities could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit any of these vulnerabilities. (CVE 2012-1864 CVE 2012-1865 CVE 2012-1866 CVE 2012-1867 CVE 2012-1868) A vulnerability exists in kernel-mode drivers which, if exploited, could give an attacker the ability to execute arbitrary program code on the vulnerable computer. (CVE 2012-0157)	**XP** **32-bit:**KB2718523 **XP** **64-bit:**KB2718523 **2003** **32-bit:**KB2718523 **2003** **64-bit:**KB2718523 **Vista** **32-bit:**KB2718523 **Vista** **64-bit:**KB2718523 **2008** **32-bit:**KB2718523 **2008** **64-bit:**KB2718523 **W7** **32-bit:**KB2718523 **W7** **64-bit:**KB2718523 **2008** **R2:**KB2718523	12-018 12-041 12-047
MS Remote Desktop Could Allow Remote Code Execution Vulnerabilities	Fixed Remote Code Execution Vulnerabilities in the Remote Desktop Protocol. If exploited, an attacker could run arbitrary code on the target system, then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE 2012-0002, CVE 2012-0152)	KB2621440 and KB2621402 **XP:** 32-bit, 64-bit **2003:** 32-bit, 64-bit, Itanium **Vista:** 32-bit, 64-bit **2008:** 32-bit, 64-bit, Itanium **2008 R2:** 64-bit(1), 64-bit(2), Itanium(1), Itanium(2) **Win 7:** 32-bit(1), 32-bit(2), 64-bit(1), 64-bit(2)	12-020
Windows Kernel Elevation of Privilege Vulnerability	Fixes a vulnerability that could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application that exploits the vulnerability. This vulnerability affects all 32-bit editions of Windows XP and Windows Server 2003: (CVE 2012-0217), and it also affects Windows 7 for x64-based Systems, and Windows Server 2008 R2 for x64-based Systems: (CVE 2012-1515)	**XP SP3:** 2707511 (32-bit) **2003 SP2:** 2707511 (32-bit) **Window 7:** 2709715 (64-bit) **2008 R2:** 2709715 (64-bit)	12-042
Windows C Run-Time Library remote code execution vulnerability	Fixes a remote code vulnerability in the way that the `msvcrt.dll` calculates	**Vista:** 2654428 (32-bit), 2654428	12-013

	the size of a buffer in memory, allowing data to be copied into memory that has not been properly allocated. This vulnerability could allow remote code execution if a user opens a specially crafted media file that is hosted on a website or sent as an email attachment. An attacker who successfully exploits the vulnerability could gain the same user rights as the local user. (CVE 2012-0150)	(64-bit) **2008:** 2654428 (32-bit), 2654428 (64-bit) **Windows 7:** 2654428 (32-bit), 2654428 (64-bit) **2008 R2:** 2654428 (64-bit)	
Windows Color Control Panel Insecure Library Loading vulnerability	Fixes a vulnerability in Windows Server 2008 and 2008 R2 that could allow remote code execution. The vulnerability is caused in the way that the Color Control Panel handles the loading of DLL files when a user opens a legitimate file (example, .icm or .icc) which is in the same directory as the specially crafted dll file. An attacker could run arbitrary code in the context of the current user. (CVE 2010-5082)	**2008:** 2643719, 2643719 (64-bit) **2008R2:** 2643719	12-012
Vulnerability in Indeo Codec	A vulnerability exists in the Indeo codec for Windows XP SP3. The vulnerability could allow remote code execution if a user opens a legitimate file from a directory which also contains a specially-crafted dll file. If successful, the attacker could then run arbitrary code as the logged-on user. The higher the privilege level of the logged-on user, the more damage could be done. (CVE 2010-3138)	**XP 32-bit SP3** 2661637	12-014
Microsoft Windows DirectWrite Denial of Service Vulnerability	Fixes a vulnerability in Windows `DirectWrite`. In an Instant Messenger-based attack scenario, the vulnerability could allow denial of service if an attacker sends a specially crafted sequence of Unicode characters directly to an Instant Messenger client. (CVE 2012-0156)	**Vista:**KB2665364 **2008:**KB2665364 **Win 7:**KB2665364	12-019 (superseded by 12-034 on all vulnerable platforms)
MS Forefront Unified Access Gateway 2010 information disclosure vulnerability	Two information disclosure vulnerabilities exist in Unified Access Gateway (UAG) 2010 SP1: A spoofing vulnerability could allow an outside attacker to acquire authentication cookies and credentials for an internal UAG user, and an access vulnerability could allow an unauthenticated attacker on the (external) Internet to acquire confidential content from a UAG server's (internal) default Web page. (CVE 2012-0146, CVE 2012-0147)	**UAG 2010 SP1:** KB2649261 **SP1 Update 1:** KB2649262	12-026
Windows Authenticode Signature Verification function bypass	The `WinVerifyTrust` function improperly validates the signature of an executable file, allowing for the	**XP:**KB2653956 **2003:**KB2653956 **Vista:**KB2653956	12-024

	potential execution of untrusted code. (CVE 2012-0151)	**Win 7:**KB2653956 **2008:**KB2653956 **2008 R2:**KB2653956	
Privilege Vulnerability fixed by MS12-033	MS12-033 fixed a Plug and Play (PnP) Configuration Manager Vulnerability in Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application. (CVE 2012-0178)	**Vista 32 bit SP2:**KB2690533, **Vista 64 bit SP2:**KB2690533 **W7 32 bit:**KB2690533, **W7 32 bit SP1:**KB2690533, **W7 64 bit:**KB2690533, **W7 64 bit SP1:**KB2690533, **2008 32 bit SP2:**KB2690533, **2008 64 bit SP2:**KB2690533, **2008 Itanium SP2:**KB2690533, **2008 R2 64 bit:**KB2690533, **2008 R2 64 bit SP1:**KB2690533, **2008 R2 Itanium:**KB2690533, **2008 R2 Itanium SP1:**KB2690533	12-033
Multiple vulnerabilities fixed by MS12-034	MS12-034 fixed multiple vulnerabilities in Windows, Office, GDI+, .NET, and Silverlight. (CVE 2011-3402 CVE 2012-0159 CVE 2012-0165 CVE 2012-0167 CVE 2012-0180 CVE 2012-0181 CVE 2012-1848)	MS12-034	12-034
Windows RDP Remote Code Execution Vulnerability (MS12-036)	MS12-036 fixed a vulnerability in the Remote Desktop Protocol which allowed for potential remote code execution. (CVE 2012-0173)	**XP SP3 (32-bit):**KB2685939 **XP SP2 (64-bit)**KB2685939 **Vista SP2 (32-bit)**KB2685939 **Vista SP2 (64-bit)**KB2685939 **7 (32-bit)**KB2685939 **7 SP1 (32-bit)**KB2685939 **7 (64-bit)**KB2685939 **7 SP1 (64-bit)**KB2685939 **2003 SP2 (32-bit)**KB2685939 **2003 SP2 (64-bit)**KB2685939	12-036

		2003 SP2 (Itanium)KB2685939 **2008 SP2 (32-bit)**KB2685939 **2008 SP2 (64-bit)**KB2685939 **2008 SP2 (Itanium)**KB2685939 **2008 R2 (64-bit)**KB2685939 **2008 R2 SP1 (64-bit)**KB2685939 **2008 R2 (Itanium)**KB2685939	
Microsoft Lync Multiple Vulnerabilities (MS12-039)	Four vulnerabilities have been patched in the following Microsoft Lync applications: Communicator 2007 R2, Lync 2010, Lync 2010 Attendee, and Lync 2010 Attendant. The vulnerabilities include two TrueType font parsing vulnerabilities, a DLL injection vulnerability, and an HTML sanitization vulnerability. (CVE 2011-3402, CVE 2012-0159, CVE 2012-1849, CVE 2012-1858)	**Communicator 2007 R2**:KB2708980 **Lync 2010**:KB2693282 **Lync 2010 Attendee**:KB2696031 **Lync 2010 Attendant**:KB2702444	12-039
MDAC ADO cachesize heap overflow	Microsoft Data Access Components (MDAC) ActiveX Data Objects (ADO) could allow command execution when parsing specially crafted XML code due to an attempt to access an uninitialized object. (CVE 2012-1891)	**XP:** 2698365 **2003:** 2698365 **Vista:** 2698365 **2008:** 2698365 **7:** 2698365 **2008 R2:** 2698365	12-045
Remote Desktop Protocol Use After Free Vulnerability	The Windows XP implementation of the Remote Desktop Protocol (RDP) contains a use-after-free vulnerability. An unauthenticated remote attacker may be able to trigger the vulnerability by sending a sequence of specially crafted messages to the RDP service. This may result in heap corruption that could lead to arbitrary code execution. (CVE 2012-2526)	**XP:** 2723135	12-053
Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution	Fixes three vulnerabilities in Microsoft Windows. The most severe of these vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a malicious webpage that embeds TrueType font files. (CVE 2012-2530 CVE 2012-2553 CVE 2012-2897) Also fixes a “use after free” coding error. The error could allow an authenticated local user to raise his privileges to administrator (or	**XP (32-bit):**KB2761226 **XP (64-bit):**KB2761226 **2003 (32-bit):**KB2761226 **2003 (64-bit):**KB2761226	12-055 12-075

	potentially even kernel) levels. (CVE2012-2527)	**Vista (32-bit):**KB2761226 **Vista (64-bit):**KB2761226 **2008 (32-bit):**KB2761226 **2008 (64-bit):**KB2761226 **Win 7 (32-bit):**KB2761226 **Win 7 (64-bit):**KB2761226 **2008 R2:**KB2761226 **Win 8 (32-bit):**KB2761226 **Win 8 (64-bit):**KB2761226 **2012:**KB2761226	
VBScript and JScript Engines JavaScript integer overflow	An integer overflow vulnerability allows command execution when a user opens a specially crafted web page in Internet Explorer or an application or document which embeds a malicious ActiveX control. (CVE 2012-2523)	**XP:** 2706045 **2003:** 2706045 **Vista:** 2706045 **2008:** 2706045 **7:** 2706045 **2008 R2:** 2706045	12-056
Windows networking components remote code execution	Multiple vulnerabilities exist in Windows remote administration protocol that can lead to remote code execution. Attackers that successfully exploit any of these vulnerabilities could take complete control of the system or cause a denial of service. (CVE 2012-1850, CVE 2012-1852, CVE 2012-1853)	**XP:** 2705219 **2003:** 2705219 **Vista:** 2705219 **2008:** 2705219 **7:** 2705219 **2008 R2:** 2705219	12-054
Windows print spooler remote code execution vulnerability	A vulnerability exists in the Windows print spooler service that can lead to remote code execution. Attackers that successfully exploit this vulnerability could take complete control of the system. (CVE 2012-1851)	**XP:** 2712808 **2003:** 2712808 **Vista:** 2712808 **2008:** 2712808 **7:** 2712808 **2008 R2:** 2712808	12-054
Windows Kernel integer overflow	Fixes a vulnerability which could allow a logged-on user to gain administrative privileges. (CVE 2012-2529)	**XP:** 2724197 **2003:** 2724197 **Vista:** 2724197 **2008:** 2724197 **7:** 2724197 **2008 R2:** 2724197	12-068

HTML Sanitization Vulnerability in Various Products	Various products do not properly validate user-supplied HTML input, which may result in a Cross Site Scripting or privilege-escalation vulnerability. An attacker could exploit this weakness to steal a user's session or other privileged information. In a web-based attack scenario, an attack could be delivered by directing the user to a target SharePoint website. Attackers may also target users of Lync 2010 and Communicator 2007 R2 by sending them a specially crafted message. (CVE 2012-2520)	**Communicator 2007 R2:** 2726391 **Lync 2010:** 2726382 **Lync 2010 Attendee:** 2726388 **SharePoint Server 2007:** 2687405 (32-bit), 2687405 (64-bit) **SharePoint Server 2010:** 2687435, 2589280 on 2010 MS Business Productivity Servers **SharePoint Server Services 3.0:** 2687356 (32-bit), 2687356 (64-bit) **SharePoint Foundation 2010:** 2687434	12-066
HTML Sanitization Vulnerability in Various Products	Various products do not properly validate user-supplied HTML input, which may result in a Cross Site Scripting or privilege-escalation vulnerability. An attacker could exploit this weakness to steal a user's session or other privileged information. In a web-based attack scenario, an attack could be delivered by directing the user to a target SharePoint website. Attackers may also target users of Lync 2010 and Communicator 2007 R2 by sending them a specially crafted message. (CVE 2013-1302)	**Communicator 2007 R2:** 2827753 **Lync 2010:** 2827750 **Lync 2010 Attendee:** 2827752	13-041
HTML Sanitization Vulnerability in Various Products	Various products do not properly validate user-supplied HTML input, which may result in a Cross Site Scripting or privilege-escalation vulnerability. An attacker could exploit this weakness to steal a user's session or other privileged information. Attackers may target users of Lync 2010 and Lync 2013 by sending them a specially crafted message. (CVE 2014-1823)	**Lync Server 2010:** 2963286 **Lync Server 2013:** 2963288	14-032
Microsoft Windows Briefcase remote code execution vulnerabilities	Fixes two privately reported vulnerabilities by modifying the way that Microsoft Windows handles a specially crafted briefcase. (CVE 2012-1527 CVE 2012-1528)	**XP:** 2727528 (32 bit), 2727528 (64 bit) **2003:** 2727528 (32 bit), 2727528 (64 bit)	12-072

		Vista: 2727528 (32 bit), 2727528 (64 bit) **2008:** 2727528 (32 bit), 2727528 (64 bit) **7:** 2727528 (32 bit), 2727528 (64 bit) **2008 R2:** 2727528 (64 bit) **8:** 2727528 (32 bit), 2727528 (64 bit) **2012:** 2727528 (32 bit)	
Vulnerability in `IP-HTTPS` Component Could Allow Security Feature Bypass	Fixes a vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass if an attacker presents a revoked certificate to an `IP-HTTPS` server commonly used in Microsoft `DirectAccess` deployments. (CVE 2012-2549)	**2008 R2:**KB2765809 **2012:**KB2765809	12-083
Vulnerability in `DirectPlay` Could Allow Remote Code Execution	Fixes a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker convinces a user to view a specially crafted Office document with embedded content. An attacker who successfully exploits this vulnerability could gain the same user rights as the current user. (CVE 2012-1537)	**XP:**KB2770660 **2003:**KB2770660 **Vista:**KB2770660 **2008:**KB2770660 **7:**KB2770660 **2008 R2 (64 bit):**KB2770660 **Window 8:**KB2770660 **2012:**KB2770660	12-082
Microsoft Windows Kernel-Mode Drivers Font Parsing Vulnerabilities	There are vulnerabilities in the handling of both “OpenType” and “TrueType” fonts, such that attempting to render characters from a specially-crafted malicious font file, even from a remote Web page, may give an attacker complete control of the victim's computer. (CVE 2012-2556, CVE 2012-4786)	KB2753842 (OT), KB2779030 (TT) **XP:** x86 (OT TT), x64 (OT TT) **2003:** x86 (OT TT), x64 (OT TT), IA64 (OT TT) **Vista:** x86 (OT TT), x64 (OT TT) **2008:** x86 (OT TT), x64 (OT TT), IA64 (OT TT) **W7:** x86 (OT TT), x64 (OT TT) **2008 R2:** x64 (OT TT), IA64 (OT TT) **W8:** x86 (OT TT), x64 (OT TT) **2012:** x64 (OT TT)	12-078
Microsoft Windows File Handling Component vulnerability	Fixes a vulnerability in Windows file handling component which could allow remote code execution if a user browses to a folder that contains a file or subfolder with a specially crafted name. An attacker who successfully	**XP:** 2758857 (32 bit), 2758857 (64 bit) **2003:** 2758857 (32 bit), 2758857 (64 bit)	12-081

	exploited this vulnerability could gain the same user rights as the current user. (CVE 2012-4774)	**Vista:** 2758857 (32 bit), 2758857 (64 bit) **2008:** 2758857 (32 bit), 2758857 (64 bit) **7:** 2758857 (32 bit), 2758857 (64 bit) **2008 R2:** 2758857 (64 bit)	
Microsoft Word RTF `listoverridecount` Vulnerability in SharePoint Server 2010 Word Automation Services	Fixes a remote code execution vulnerability due to an error in the way the `/listoverridecount` RTF header is parsed. (CVE 2012-2539)	**SharePoint 2010:** 2760405	12-079
Microsoft Exchange Server RSS feed denial of service	Fixes a vulnerability in the way Microsoft Exchange Server 2010 and 2007 handle RSS feeds that could lead to a denial of service. Fixes a vulnerability in Oracle Outside due to a remote code execution vulnerability in the WebReady Document Viewing feature of Microsoft Exchange Server. (CVE 2012-3214, CVE 2012-3217, CVE 2012-4791)	**Patch:** MS12-080	12-080
Kernel-Mode Driver Privilege Escalation Vulnerability	Fixes a vulnerability caused by improper handling of windows broadcast messages by the Windows kernel. The vulnerability could allow an attacker to gain full control of the effected system. (CVE 2013-0008)	**Vista:** 2778930 (32 bit), 2778930 (64 bit) **Server 2008:** 2778930 (32 bit), 2778930 (64 bit), 2778930 (IA64) **Windows 7:** 2778930 (32 bit), 2778930 (64 bit) **Server 2008 R2:** 2778930 (64 bit), 2778930 (IA64) **Windows 8:** 2778930 (32 bit), 2778930 (64 bit) **Server 2012:** 2778930	13-005
Windows print spooler remote code execution vulnerability	A vulnerability exists in the Windows print spooler service that can lead to remote code execution. Attackers that successfully exploit this vulnerability could take complete control of the system. (CVE 2013-0011)	**Windows 7:** 2769369 **2008 R2:** 2769369	13-001
Windows TCP FIN WAIT Vulnerability	Fixes a vulnerability in the way that Microsoft Windows handles TCP FIN responses when window size is equal to zero. (CVE 2013-0075)	**Vista SP2:** 2790655 **Vista (x64) SP2:** 2790655 **2008 (x86) SP2:** 2790655 **2008 (x64) SP2:** 2790655 **Windows 7 (x86):**	13-018 (superseded by 13-049 on all vulnerable platforms)

		2790655 **Windows 7 (x64):** 2790655 **Windows 7 SP1 (x86):** 2790655 **Windows 7 SP1 (x64):** 2790655 **2008 R2 (x64):** 2790655 **2008 R2 SP1 (x64):** 2790655 **Windows 8 (x32):** 2790655 **Windows 8 (x64):** 2790655 **2012 (x64) SP2:** 2790655	
Windows TCP Kernel Mode Driver Vulnerability	Fixes a vulnerability in the way that Microsoft Windows handles TCP packets during a connection. (CVE 2013-3138)	**Vista SP2:** 2845690 **Vista (x64) SP2:** 2845690 **2008 (x86) SP2:** 2845690 **2008 (x64) SP2:** 2845690 **Windows 7 SP1 (x86):** 2845690 **Windows 7 SP1 (x64):** 2845690 **2008 R2 (x64) SP1:** 2845690 **Windows 8 (x32):** 2845690 **Windows 8 (x64):** 2845690 **2012 (x64) SP2:** 2845690	13-049
SSL Version 3 and TLS Security Feature Bypass	Fixes a vulnerability in the way that Microsoft Windows SSL/TLS handle the SSL version 3 (SSLv3) and TLS protocols. The vulnerability could allow security feature bypass if an attacker injects specially crafted content into an SSL/TLS session. (CVE 2013-0013)	**Vista:** 2785220 (32 bit), 2785220 (64 bit) **Server 2008:** 2785220 (32 bit), 2785220 (64 bit) **Windows 7:** 2785220 (32 bit), 2785220 (64 bit) **2008 R2:** 2785220 **Windows 8:** 2785220 (32 bit), 2785220 (64 bit) **2012:** 2785220	13-006
Windows Kernel integer overflow	Fixes a vulnerability which could allow a logged-on user to gain administrative privileges. (CVE 2013-1278) (CVE 2013-1279) (CVE 2013-1280)	**XP:** 2799494 **2003:** 2799494 **Vista:** 2799494 **2008:** 2799494 **7:** 2799494 **2008 R2:**	13-017

		2799494 **8:** 2799494 **2012:** 2799494	
Windows DirectShow Media Decompression vulnerability fixed by MS13-011	Fixes a vulnerability which could allow remote code execution if a user opens a specially crafted media file (such as an **.mpg** file), opens a Microsoft Office document (such as a **.ppt** file) that contains a specially crafted embedded media file, or receives specially crafted streaming content. (CVE 2013-0077)	**XP:** 2780091 (32-bit), 2780091 (64-bit) **2003:** 2780091 (32-bit), 2780091 (64-bit) **Vista:** 2780091 (32-bit), 2780091 (64-bit) **2008:** 2780091 (32-bit), 2780091 (64-bit)	13-011
Kernel-Mode Driver Elevation Of Privilege Vulnerabilities	This security update resolves three privately reported vulnerabilities and one publicly disclosed vulnerability in Microsoft Windows. The most severe of these vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. (CVE 2013-1283 CVE 2013-1291 CVE 2013-1292 CVE 2013-1293)	**XP:** 2808735 (32 bi1t) **Server 2003:** 2808735 (32 bit) **Vista:** 2808735 (32 bit) **Server 2008:** 2808735 (32 bit) **Windows 7:** 2808735 (32 bit) **Windows 8:** 2808735 (32 bit)	13-036
Kernel-Mode Driver Privilege Escalation Vulnerabilities	This security update resolves 30 privately reported vulnerabilities in Microsoft Windows. These vulnerabilities exist when the Windows kernel-mode driver improperly handles objects in memory. An attacker who successfully exploited these vulnerabilities could gain elevated privileges and read arbitrary amounts of kernel memory. An attacker must have valid logon credentials and be able to log on locally to exploit these vulnerabilities. (CVE 2013-1248 CVE 2013-1249 CVE 2013-1250 CVE 2013-1251 CVE 2013-1252 CVE 2013-1253 CVE 2013-1254 CVE 2013-1255 CVE 2013-1256 CVE 2013-1257 CVE 2013-1258 CVE 2013-1259 CVE 2013-1260 CVE 2013-1261 CVE 2013-1262 CVE 2013-1263 CVE 2013-1264 CVE 2013-1265 CVE 2013-1266 CVE 2013-1267 CVE 2013-1268 CVE 2013-1269 CVE 2013-1270 CVE 2013-1271 CVE 2013-1272 CVE 2013-1273 CVE 2013-1274 CVE 2013-1275 CVE 2013-1276 CVE 2013-1277)	**XP:** 2778344 (32 bit), 2778344 (64 bit) **Server 2003:** 2778344 (32 bit), 2778344 (64 bit) **Vista:** 2778344 (32 bit), 2778344 (64 bit) **Server 2008:** 2778344 (32 bit), 2778344 (64 bit) **Windows 7:** 2778344 (32 bit), 2778344 (64 bit) **Server 2008 R2:** 2778344 (64 bit)	13-016
Windows CSRSS Privilege Elevation Vulnerability	Fixes a vulnerability which might allow an authenticated user to execute arbitrary code in the context of the	**Windows 7:** 2790113 (32-bit), 2790113 (64-bit)	13-019

	local system. (CVE 2013-0076)	**Server 2008 R2:** 2790113 (64-bit), 2790113 (IA64)	
Windows NFS Server null dereference vulnerability	Fixes a denial of service vulnerability in the Windows NFS server when handling a file operation on a read-only share. (CVE 2013-1281)	**2008 R2:** 2790978 **2012:** 2790978	13-014
Windows OLE Automation Remote Code Execution Vulnerability	This update corrects a memory corruption vulnerability in the Object Linking and Embedding (OLE) Automation library. (CVE 2013-1313)	**Windows XP:** 2802968	13-020
Windows RDP ActiveX Control vulnerability	Fixes a use-after-free vulnerability in the Remote Desktop ActiveX control which could allow command execution when a user browses to a malicious web site. (CVE 2013-1296)	**XP (RDP 6.1):** 2813345 **XP (RDP 7.0):** 2813347 **2003:** 2813345 **Vista (RDP 6.1):** 2813345 **Vista (RDP 7.0):** 2813347 **2008:** 2813345 **7:** 2813347 **2008 R2:** 2813347	13-029
Two Windows RDP vulnerabilities	Fixes two RDP vulnerabilities: (1) a remote desktop session host spoofing vulnerability in Windows Vista, Server 2008, 7, Server 2008 R2, 8, Server 2012, 8.1 and Server 2012 R2 that could allow host spoofing via a man-in-the-middle attack; and (2) a remote code execution vulnerability in Windows 7 and Server 2008 R2 that would require an attacker to place a specially crafted DLL file in the target user's current working directory and then convince the user to open a specially crafted RDP file. (CVE 2015-2472, CVE 2015-2473)	**Vista (RDP 6.1):** 3075220 **Vista (RDP 7.0):** 3075221 **Server 2008:** 3075220 32-bit, 3075220 64-bit **7 (no RDP):** 3075220 32-bit, 3075220 64-bit **7 (RDP 8.0):** 3075222 32-bit, 3075222 64-bit **7 (RDP 8.1):** 3075226 32-bit, 3075226 64-bit **Server 2008 R2 (no RDP):** 3075220 **Server 2008 R2 (RDP 8.0):** 3075222 **Server 2008 R2 (RDP 8.1):** 3075226 **8:** 3075220 32-bit, 3075220 34-bit **Server 2012:** 2813347 **8.1:** 3075220 32-bit, 3075220 34-bit **Server 2012 R2:** 2813347	15-082

Windows Kernel Race Condition Vulnerabilities	This update resolves two privately reported vulnerabilities that could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit these vulnerabilities. (CVE 2013-1284, CVE 2013-1294)	**XP:** 2813170 (32 bit), 2813170 (64 bit) **2003:** 2813170 (32 bit), 2813170 (64 bit) **Vista:** 2813170 (32 bit), 2813170 (64 bit) **2008:** 2813170 (32 bit), 2813170 (64 bit) **7:** 2813170 (32 bit), 2813170 (64 bit) **2008 R2:** 2813170 **8:** 2813170 (32 bit), 2813170 (64 bit) **2012:** 2813170	13-031
DirectX Graphics Kernel Subsystem Double Fetch Vulnerability	Fixes a vulnerability which could allow a logged-in user to gain elevated privileges. (CVE 2013-1332)	**Vista:** 2830290 **2008:** 2830290 **7:** 2830290 **2008 R2:** 2830290 **8:** 2830290 **2012:** 2830290	13-046
Win32k vulnerabilities	Fixes two vulnerabilities, one in Windows XP and one in Windows 7, which could allow a logged-in user to elevate privileges. (CVE 2013-1333 CVE 2013-1334)	**XP:** 2829361 **7:** 2829361	13-046
Windows print spooler privilege elevation vulnerability	When a printer connection is deleted, the Windows Print Spooler does not properly free memory, exposing a vulnerability through which an authenticated user could elevate their privileges. (CVE 2013-1339)	KB2839894 **Vista:** 32 bit, 64 bit **2008:** 32 bit, 64 bit, Itanium **Win 7:** 32 bit, 64 bit **2008 R2:** 64 bit, Itanium **Win 8:** 32 bit, 64 bit **2012:** 64 bit	13-050
Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	This security update resolves multiple vulnerabilities in Microsoft Windows. The most severe vulnerabilities could allow elevation of privilege if an attacker logged on locally and ran a specially crafted application. (CVE 2013-2556 CVE 2013-3196 CVE 2013-3197 CVE 2013-3198) This security update also resolves one privately reported vulnerability in Windows. This vulnerability could allow information disclosure if an attacker logs on to a system and runs a	**XP:**KB2859537 **Server 2003:**KB2859537 **Vista:**KB2859537 **Vista x64:**KB2859537 **Server 2008:**KB2859537 **Server 2008 x64:**KB2859537 **7:**KB2859537 **7 x64:**KB2859537 **Server 2008**	13-048 13-063

	specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. (CVE 2013-3136)	R2:KB2859537 **8:**KB2859537	
Microsoft Windows Media Format Runtime Remote Code Execution Vulnerability	This security update resolves one vulnerability in Windows. The vulnerability could allow remote code execution if a user opens a specially crafted media file. (CVE 2013-3127)	**XP: Windows Media Format Runtime 11:**KB2834904 **XP: Windows Media Format Runtime 9.5:**KB2834905 **XP: Windows Media Format Runtime 9:**KB2803821 **XP: Windows Media Format Runtime 9.5:**KB2834902 **XP: Windows Media Format Runtime 9.5:**KB2834903 **XP: Windows Media Format Runtime 11:**KB2834904 **XP: wmv9vcm.dll (codec):**KB2845142 **XP x64: Windows Media Format Runtime 9.5:**KB2803821 **XP x64: Windows Media Format Runtime 9.5 x64:**KB2834902 **XP x64: Windows Media Format Runtime 11:**KB2834904 **XP x64: wmv9vcm.dll (codec):**KB2845142 **2003: Windows Media Format Runtime 9.5:**KB2803821 **2003: wmv9vcm.dll (codec):**KB2845142 **2003 x64: Windows Media**	13-057

Format Runtime 9.5:KB2803821
2003 x64: Windows Media Format Runtime 9.5 x64:KB2834902
2003 x64: Windows Media Format Runtime 11:KB2834904
2003 x64: wmv9vcm.dll (codec):KB2845142
Vista: Windows Media Player 11:KB2803821
Vista: wmv9vcm.dll (codec):KB2845142
Vista x64: Windows Media Player 11:KB2803821
Vista x64: wmv9vcm.dll (codec):KB2845142
2008: Windows Media Player 11:KB2803821
2008: wmv9vcm.dll (codec):KB2845142
2008 x64: Windows Media Player 11:KB2803821
2008 x64: wmv9vcm.dll (codec):KB2845142
Win 7: Windows Media Player 12:KB2803821
Win 7 x64: Windows Media Player 12:KB2803821
2008 R2: Windows Media Player 12:KB2803821
Win 8: Windows Media Player

		12:KB2803821 **Win 8 x64: Windows Media Player 12:**KB2803821 **2012: Windows Media Player 12:**KB2803821	
Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution	This security update resolves multiple vulnerabilities in Microsoft SharePoint Server. The most severe vulnerabilities could result in remote code execution. (CVE 2013-0081 CVE 2013-1330 CVE 2013-3179 CVE 2013-3180)	**Microsoft SharePoint 2007 and Services 3.0 (x86 & 64bit):**KB2760420 **SharePoint Server 2010 (SP1 & SP2):**KB2810067 **SharePoint Server 2013:**KB2760420	13-067
SharePoint Page Content Vulnerabilities	This security update resolves multiple vulnerabilities in Microsoft SharePoint Server, and Microsoft Office Services and Web Apps hosted on SharePoint Server. Successful exploitation of these vulnerabilities could result in remote code execution. (CVE 2013-5059)	**2010 Business Productivity Servers (SharePoint Server 2010 SP1 & SP2):** KB2553298 **SharePoint Enterprise Server 2013 (SharePoint Server 2013):** KB2837629 and KB2837631 **Microsoft Office Web Apps Server 2013 (SharePoint Server 2013):** KB2910228	13-100
GDI+ TrueType Font Parsing vulnerability	Fixes a vulnerability in Windows, Office, Visual Studio, and Lync which could allow command execution when a user loads an attacker's web page or opens a specially crafted file or application. (CVE 2013-3129)	13-054	13-054
Windows Kernel-Mode Drivers remote code execution vulnerabilities	This security update resolves two publicly disclosed and six privately reported vulnerabilities in Microsoft Windows. The most severe vulnerability could allow remote code execution if a user views shared content that embeds TrueType font files. (CVE 2013-1300 CVE 2013-1340 CVE 2013-1345 CVE 2013-3129 CVE 2013-3167 CVE 2013-3172 CVE 2013-3173 CVE 2013-3660)	KB2850851 **XP:** 32 bit, 64 bit **2003:** 32 bit, 64 bit, Itanium **Vista:** 32 bit, 64 bit **2008:** 32 bit, 64 bit, Itanium **Win 7:** 32 bit, 64 bit **2008 R2:** 64 bit, Itanium **Win 8:** 32 bit, 64 bit **2012:** 64 bit	13-053

Windows DirectShow Remote Code Execution Vulnerability	This update resolves a Remote Code Execution Vulnerability in Microsoft DirectShow. The vulnerability can be triggered if an attacker submits a crafted GIF file and an user opens it. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. (CVE 2013-3174)	**XP:** 2845187 (32 bit) **2003:** 2845187 (32 bit) **Vista:** 2845187 (32 bit) **2008:** 2845187 (32 bit) **7:** 2845187 (32 bit) **2008 R2:** 2845187 (64 bit) **8:** 2845187 (32 bit) **2012:** 2845187	13-056 (superseded by MS14-013)
OLE Remote Code Execution Vulnerability	Fixes a remote code execution vulnerability in OLE triggered when a user opens a file that contains a specially crafted OLE object. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. (CVE 2013-3863)	**XP:** 2876217 (32 bit), 2876217 (64 bit) **2003:** 2876217 (32 bit), 2876217 (64 bit), Itanium	13-070
Windows DirectShow Privilege Elevation Vulnerability	The MS14-041 update addresses a privilege elevation vulnerability in Microsoft Windows DirectShow. The vulnerability would allow a low privilege process to elevate to the permissions of the logged in user. (CVE 2014-2780)	**Vista:** 2972280(32 bit), 2972280(64 bit) **2008:** 2972280(32 bit), 2972280(64 bit) **7:** 2972280(32 bit), 2972280(64 bit) **2008 R2:** 2972280 **8:** 2972280(32 bit), 2972280(64 bit) **8.1:** 2972280(32 bit), 2972280(64 bit) **2012:** 2972280 **2012 R2:** 2972280	14-041
Windows TCP/IP Window Resize Vulnerability	The MS14-031 update addresses a denial of service vulnerability in the Windows TCP/IP stack that results from improper parameter validation incoming TCP packets. (CVE 2014-1811)	**Vista:** 2957189 (32 bit), 2957189 (64 bit) **2008:** 2957189 (32 bit), 2957189 (64 bit) **7:** 2957189 (32 bit), 2957189 (64 bit) **2008 R2:** 2957189 **8:** 2957189 (32 bit), 2957189 (64 bit) **2012:** 2957189 **8.1:** This update is available via Windows Update	14-031

		only. **2012 R2:** 2957189	
Windows TCP/IP Stack ICMPv6 Memory Allocation Vulnerability	The MS13-065 update addresses a denial of service vulnerability in the Windows TCP/IP stack that results from improper memory allocation for incoming ICMPv6 packets. (CVE 2013-3183)	**Vista:** 2868623 (32 bit), 2868623 (64 bit) **2008:** 2868623 (32 bit), 2868623 (64 bit) **7:** 2868623 (32 bit), 2868623 (64 bit) **2008 R2:** 2868623 **8:** 2868623 (32 bit), 2868623 (64 bit) **2012:** 2868623	13-065
Windows Vulnerability in Unicode Script Processor	This update resolves memory corruption vulnerability in the Unicode Scripts Processor which is included in affected versions of Microsoft Windows XP and Windows Server 2003. The vulnerability could allow remote code execution if a user viewed a specially crafted document or Web page with an application that supports embedded OpenType fonts. (CVE 2013-3181)	**XP:** 2850869 (32 bit), 2850869 (64 bit). **2003:** 2850869 (32 bit), 2850869 (64 bit).	13-060
Microsoft Exchange Server Oracle Outside Remote Code Execution Vulnerabilities	Fixes three vulnerabilities in Oracle Outside for Microsoft Exchange Server 2007, 2010, and 2013 that could allow attackers to execute arbitrary code. (CVE 2013-2393 CVE 2013-3776 CVE 2013-3781)	**2007 SP3:** 2873746 **2010 SP2:** 2874216 **2010 SP3:** 2866475 **2013 Update 1:** 2874216 **2013 Update 2:** 2874216	13-061
Windows Theme File Could Allow Remote Code Execution Vulnerability	This security update addresses a privately reported vulnerability in Microsoft Windows that could allow remote code execution if a user inadvertently applies a specially crafted Windows theme on their system. Fortunately, a user cannot be forced to open the file or apply the theme in order for this attack to be successful, a user must be convinced to do so. (CVE 2013-0810)	**XP** 2864063 (32 bit), 2864063 (64 bit) **2003** 2864063 (32 bit), 2864063 (64 bit) **Vista** 2864063 (32 bit), 2864063 (64 bit) **2008** 2864063 (32 bit), 2864063 (64 bit)	13-071
Active Directory Federation Services Information Disclosure Vulnerability	This security update resolves a vulnerability in Active Directory Federation Services (AD FS). The vulnerability could reveal information pertaining to the service account used by AD FS. A malicious user could then attempt logons externally resulting in an account lockout of the service	**2003:** 2868864 (32 bit) 2868864 (64 bit) **2008:** 2868864 (32 bit) 2868864 (32 bit) 2868864 (64 bit) 2868864 (64 bit)	13-066

	account used by AD FS. This would ultimately result in a denial of service for all applications relying on the AD FS instance. (CVE 2013-3185)	**2008 R2:** 2868864 (64 bit) 2868864 (64 bit) **2012:** 2868864 (32 bit)	
Windows Kernel-Mode Drivers multiple elevation of privilege vulnerabilities	This security update resolves seven privately reported vulnerabilities in Microsoft Windows. These vulnerabilities exist due to the way Windows kernel-mode driver improperly handles objects in memory. An attacker who successfully exploited these vulnerabilities could gain elevated privileges and read arbitrary amounts of kernel memory. (CVE 2013-1341 CVE 2013-1342 CVE 2013-1343 CVE 2013-1344 CVE 2013-3864 CVE 2013-3865 CVE 2013-3866)	KB2876315 **XP:** 32 bit, 64 bit **2003:** 32 bit, 64 bit, Itanium **Vista:** 32 bit, 64 bit **2008:** 32 bit, 64 bit, Itanium **Win 7:** 32 bit, 64 bit **2008 R2:** 64 bit, Itanium **Win 8:** 32 bit, 64 bit **2012:** 64 bit	13-076
Windows SCM Privilege Elevation Vulnerability	Fixes a vulnerability which might allow an authenticated user to execute arbitrary code in the context of the local system. (CVE 2013-3862)	**Windows 7:** 2872339 (32-bit), 2872339 (64-bit) **Server 2008 R2:** 2872339 (64-bit), 2872339 (IA64)	13-077
Windows Common Control Library Integer Overflow Vulnerability	MS13-083 fixes a vulnerability which could allow remote code execution if an attacker sends a specially crafted web request to an ASP.NET web application running on an affected system. The vulnerability can only be exposed through a vulnerable web application using the **`DSA_InsertItem`** function, which accepts an arbitrary user value as an argument to the function. (CVE 2013-3195)	**XP:** 2864058 (64-bit) **2003:** 2864058 (32-bit), 2864058 (64-bit) **Vista:** 2864058 (32-bit), 2864058 (64-bit) **2008:** 2864058 (32-bit), 2864058 (64-bit) **Win 7:** 2864058 (32-bit), 2864058 (64-bit) **2008 R2:** 2864058 (64-bit) **Win 8:** 2864058 (32-bit), 2864058 (64-bit) **2012:** 2864058 (64-bit)	13-083
MS Windows AD/LDAP Remote Anonymous DoS vulnerability	Fixes a vulnerability which might allow an anonymous (unauthenticated) attacker to halt the LDAP service by sending a specially-crafted malicious query. (CVE 2013-3868)	KB2853587 **Vista:** 32-bit, 64-bit **2008:** 32-bit, 64-bit **Win 7:** 32-bit, 64-bit **2008 R2:** 64-bit **Win 8:** 32-bit, 64-bit **2012:** 64-bit	13-079
Windows Kernel-Mode Drivers remote code execution	Fixes several vulnerabilities in Windows Kernel-Mode drivers that could lead to privilege elevation and	Apply patches referenced in MS13-081	13-081

	remote code execution. (CVE 2013-3128 CVE 2013-3200 CVE 2013-3879 CVE 2013-3880 CVE 2013-3881 CVE 2013-3888 CVE 2013-3894)		
Cumulative Security Update of ActiveX Kill Bits (MS13-090)	MS13-090 fixes a vulnerability in `InformationCardSigninHelper` Class ActiveX control. The vulnerability could allow remote code execution if a user views a specially crafted webpage, instantiating the ActiveX control. (CVE 2013-3918)	KB2900986 **XP:** 32-bit, 64-bit **2003:** 32-bit, 64-bit **Vista:** 32-bit, 64-bit **Windows 2008:** 32-bit, 64-bit **Windows 7:** 32-bit, 64-bit **Server 2008 R2:** 64-bit **Windows 8:** 32-bit, 64-bit **Server 2012:** 64-bit **Server 2012 R2:** 64-bit	13-090
Windows GDI Write file integer overflow	Fixes a vulnerability which could allow command execution when a user opens a specially crafted Windows Write file in Wordpad. (CVE 2013-3940)	**XP:** 2876331 **2003:** 2876331 **Vista:** 2876331 **2008:** 2876331 **7:** 2876331 **2008 R2:** 2876331 **8:** 2876331 **8.1:** 2876331 **2012:** 2876331 **2012 R2:** 2876331	13-089
Microsoft Hyper-V privilege elevation vulnerability	Fixes a privilege elevation vulnerability in Microsoft Hyper-V for Windows 8 and Windows 2012 that allows attackers to execute arbitrary code or cause a denial of service. (CVE 2013-3898)	KB2893986 **Win 8:** 64-bit **2012:** 64-bit	13-092
Windows Digital Signature vulnerability (MS13-095)	MS13-095 fixes a digital signature vulnerability in Microsoft Windows as a result of Windows not properly validating a X.509 certificate. A remote attacker who sends a specially crafted X.509 certificate to a vulnerable web service could cause the affected web service to become unresponsive. (CVE 2013-3869)	KB2868626 **XP:** 32-bit, 64-bit **2003:** 32-bit, 64-bit **Vista:** 32-bit, 64-bit **Server 2008:** 32-bit, 64-bit **Win 7:** 32-bit, 64-bit **Server 2008 R2:** 64-bit **Win 8:** 32-bit, 64-bit **Win 8.1:** 32-bit, 64-bit **Server 2012:** 64-bit **Server 2012 R2:** 64-bit	13-095

Microsoft Scripting Runtime Object Library use-after-free vulnerability	Fixes a vulnerability which could allow command execution by a web page containing specially crafted script. (CVE 2013-5056)	**XP:** 2892075 **2003 (Windows Script 5.6)**: 2892076 **2003 (Windows Script 5.7)**: 2892075 **Vista**: 2892075 **2008**: 2892075 **7**: 2892074 **2008 R2**: 2892074 **8**: 2892074 **8.1**: 2892074 **2012**: 2892074 **2012 R2**: 2892074	13-099
Windows Kernel-Mode Drivers multiple elevation of privilege vulnerabilities	This security update resolves five privately reported vulnerabilities in Microsoft Windows. The update addresses the vulnerabilities, adjusting the way that the windows kernel-mode driver validates memory address values. (CVE 2013-3899 CVE 2013-3902 CVE 2013-3903 CVE 2013-3907 CVE 2013-5058)	KB2880430 **XP:** 32 bit, 64 bit **2003:** 32 bit, 64 bit **Vista:** 32 bit, 64 bit **2008:** 32 bit, 64 bit **Win 7:** 32 bit, 64 bit **2008 R2:** 64 bit **Win 8:** 32 bit, 64 bit **Win 8.1:** 32 bit, 64 bit **2012:** 64 bit	13-101 (superseded by 14-015 on Windows 7 and Windows Server 2008 R2)
Windows kernel NDProxy privilege elevation vulnerability MS14-002	Fixes a privilege elevation vulnerability that exists due to improper validation of input passed from user mode to kernel. (CVE 2013-5065)	**XP:** 2914368 (32-bit) 2914368 (64-bit) **2003:** 2914368 (32-bit) 2914368 (64-bit)	14-002
Microsoft Graphics Component Remote Code Execution Vulnerability	Fixes a vulnerability in certain Windows components that incorrectly handle TIFF files, allowing attackers to execute remote code and potentially take over the entire system. (CVE 2013-3906)	**Vista:** 2901674 (32-bit) 2901674 (64-bit) **2008:** 2901674 (32-bit) 2901674 (64-bit) **Lync 2010:** 289937 (32-bit) 2899397 (64-bit) **Lync 2010 Attendee:** 2899393 (user level) 2899395 (admin level) **Lync 2013:** 2850057 (32-bit) 2850057 (64-bit) **Lync 2013 Basic:** 2850057 (32-bit) 2850057 (64-bit)	13-096
Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	This resolves a reported vulnerability in Microsoft Windows that could allow elevation of privilege if a attacker logs on to a system and runs a specially	KB2913602 **Win 7:** (32-bit) (64-bit)	14-003 (superseded by 14-015 on all vulnerable

	crafted application. (CVE 2014-0262)	**2008 R2:** (64-bit)	platforms)
Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure	This security update resolves a publicly disclosed vulnerability in Microsoft XML Core 3.0 Services included in various versions of Microsoft Windows. The vulnerability could allow information disclosure if a user views a specially crafted webpage using Internet Explorer. (CVE 2014-0266)	KB2916036 **Windows XP:** (32-bit), (64-bit) **Windows 2003:** (32-bit), (64-bit) **Windows Vista:** (32-bit), (64-bit) **Windows 2008 R2:** (64-bit) **Windows 8:** (32-bit), (64-bit) **Windows 8.1:** (32-bit), (64-bit) **Windows Server 2012** (64-bit) **Windows Server 2012 R2** (64-bit)	14-005 (superseded by 14-033 for all supported platforms, i.e., not XP)
Windows DirectShow JPEG file handling memory corruption vulnerability	Microsoft DirectShow is vulnerable to memory corruption due to not properly handling specially crafted JPEG image files. An attacker would need to entice the user into visiting a website with specially crafted content that could exploit this vulnerability, or by enticing the user to open a specially crafted JPEG file sent as an e-mail attachment. A successful attacker could run arbitrary code in the context of the current user. (CVE 2014-0301)	KB2929961 **Windows XP:** (32-bit), (64-bit) **Windows Server 2003:** (32-bit), (64-bit) **Windows Vista:** (32-bit), (64-bit) **Windows Server 2008:** (32-bit) (64-bit) **Windows 7:** (32-bit), (64-bit) **Windows 2008 R2:** (64-bit) **Windows 8:** (32-bit), (64-bit) **Windows 8.1:** (32-bit), (64-bit) **Windows Server 2012** (64-bit) **Windows Server 2012 R2** (64-bit)	14-013
Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass	The Microsoft SAMR service fails to properly check and update the account "locked" status. By utilizing functions of the SAMR service an attacker could brute force account passwords. (CVE 2014-0317)	KB2929961 **Windows XP:** (32-bit), (64-bit) **Windows Server 2003:** (32-bit), (64-bit) **Windows Server 2003 (AD Application**	14-016

		Mode): (32-bit), (64-bit) **Windows Vista:** (32-bit), (64-bit) **Windows Server 2008:** (32-bit), (64-bit) **Windows 2008 R2:** (64-bit) **Windows Server 2012** (64-bit) **Windows Server 2012 R2** (64-bit)	
Microsoft Direct2D remote code execution vulnerability (MS14-007)	This resolves a vulnerability in Microsoft Windows Direct2D that could allow remote code execution if a user views specially crafted files via Internet Explorer. (CVE 2014-0263)	KB2912390 **Win 7:** (32-bit) (64-bit) **2008 R2:** (64-bit) **Win 8:** (32-bit) (64-bit) **Win 8.1:** (32-bit) (64-bit) **Win 2012:** (64-bit) **Win 2012 R2:** (64-bit)	14-007
Windows TCP/IPv6 Denial of Service Vulnerability (MS14-006)	This update resolves a vulnerability in Microsoft Windows implementation of TCP/IP version 6. The vulnerability could allow a denial of service if an attacker sends a large number of specially crafted IPv6 packets to an affected system. (CVE 2014-0254)	KB2904659 **Windows 8:** (32-bit) (64-bit) **Windows Server 2012:** (64-bit)	14-006
Windows Kernel-Mode Drivers multiple elevation of privilege vulnerabilities	This security update resolves five privately reported vulnerabilities in Microsoft Windows. The update addresses the vulnerabilities, adjusting the way that the windows kernel-mode driver validates memory address values. (CVE 2014-0300 CVE 2014-0323)	KB2930275 **XP:** 32 bit, 64 bit **2003:** 32 bit, 64 bit **Vista:** 32 bit, 64 bit **2008:** 32 bit, 64 bit **Win 7:** 32 bit, 64 bit **2008 R2:** 64 bit **Win 8:** 32 bit, 64 bit **Win 8.1:** 32 bit, 64 bit **2012 and 2012 R2:** 64 bit	14-015
Windows File Handling Component Could Allow Remote Code Execution Vulnerability (MS14-019)	The update addresses this issue by correcting how Windows processes .bat and .cmd files when they are ran from within the network. The vulnerability could allow an attacker to	KB2922229 **XP:** 32 bit, 64 bit **2003:** 32 bit, 64 bit **Vista:** 32 bit, 64 bit **2008:** 32 bit, 64 bit	14-019 (superseded by 15-063)

	perform remote code execution if a user unknowingly executes specially crafted .bat and .cmd files from a trusted or semi-trusted area of the network. (CVE 2014-0315)	**Win 7:** 32 bit, 64 bit **2008 R2:** 64 bit **Win 8:** 32 bit, 64 bit **Win 8.1:** 32 bit, 64 bit **2012:** 64 bit **2012 R2:** 64 bit	
Microsoft XML Core Services Entity URI Vulnerability (MS14-033)	The MS14-033 security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability is a result of not properly enforcing user access controls when Microsoft XML Core Services (MSXML) parses XML content. Successful exploitation of this vulnerability could allow information disclosure if a logged on user visits a website that contains specially crafted content that is designed to invoke MSXML through Internet Explorer. (CVE 2014-1816)	KB2939576 **Server 2003:** 32 bit, 64 bit **Vista:** 32 bit, 64 bit **Server 2008:** 32 bit, 64 bit **7:** 32 bit, 64 bit **Server 2008 R2:** 64 bit **8:** 32 bit, 64 bit **8.1:** 32 bit, 64 bit for systems that already have the KB2918355 April 2014 cumulative update installed. (See the Update FAQ if managing updates using Windows Server Update Services, Windows Intune, or System Center Configuration Manager.) **Server 2012:** 64 bit **Server 2012 R2:** 64 bit for systems that already have the KB2918355 April 2014 cumulative update installed. (See the Update FAQ if managing updates using Windows Server Update Services, Windows Intune, or System Center Configuration Manager.) KB2957482 **Server 2003:** 32 bit, 64 bit, requires pre-installation of MSXML 6.0 RTM, MSXML 6.0	14-033

		Service Pack 1, or MSXML 6.0 Service Pack 2.	
Vulnerabilities in iSCSI Could Allow Denial of Service (MS14-028)	This security update resolves two privately reported vulnerabilities in Microsoft Windows. The vulnerabilities could allow denial of service if an attacker sends large amounts of specially crafted iSCSI packets over the target network. This vulnerability only affects servers for which the iSCSI target role has been enabled. (CVE 2014-0255 CVE 2014-0256)	KB2933826 **2008 R2:** 64 bit **2012:** 64 bit The 2933826 update is for Windows 2012 R2 systems that already have the 2919355 update installed: **2012 R2:** 64 bit KB2962073 The 2962073 update is for Windows 2012 R2 systems without the 2919355 update installed: **2012 R2:** 64 bit	14-028
Vulnerability in Group Policy Preferences (MS14-025)	This security update resolves a publicly disclosed vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if Active Directory Group Policy preferences are used to distribute passwords across the domain - a practice that could allow an attacker to retrieve and decrypt the password stored with Group Policy preferences. (CVE 2014-1812)	KB2928120 **Vista:** 32 bit 64 bit **2008:** 32 bit 64 bit **Win 7:** 32 bit 64 bit **Win 8:** 32 bit 64 bit **Win 2012:** 64 bit The 2928120 update is for Windows 8.1 and Windows 2012 R2 systems that already have the 2919355 update installed: **Win 8.1:** 32 bit 64 bit **Win 2012 R2:** 64 bit KB2961899 The 2961899 update is for Windows 8.1 and Windows 2012 R2 systems that do not have the 2919355 update installed: **Win 8.1:** 32 bit 64 bit **Win 2012 R2:** 64 bit	14-025
SharePoint and SharePoint Foundation Server vulnerability could allow cross site scripting (MS14-050)	This security update resolves a vulnerability in Microsoft SharePoint and SharePoint Foundation Server 2013. The vulnerability is a cross site	**SharePoint & SharePoint Foundation 2013:** KB2880994	14-050

	scripting vulnerability due to insufficient parameter sanitization. To exploit this vulnerability an attacker must be able to authenticate on the target SharePoint site (unless the site is configured to allow anonymous users). (CVE 2014-2816)		
SharePoint and SharePoint Designer vulnerabilities could allow remote code execution (MS14-022)	This security update resolves multiple vulnerabilities in Microsoft SharePoint and SharePoint Designer 2007, 2010, and 2013. These vulnerabilities fall into two general categories: page content and XSS. To exploit any of these related vulnerabilities, an attacker must be able to authenticate on the target SharePoint site (unless the site is configured to allow anonymous users). (CVE 2014-0251 CVE 2014-1754)	**SharePoint 2007:** KB2596763 32-bit, KB2596763 64-bit, KB2596902 32-bit, KB2596902 64-bit, KB2837616 32-bit, KB2837616 64-bit **SharePoint 2010:** KB2837588, KB2837598 **SharePoint 2010:** KB2863856, KB2863863 **SharePoint Designer 2007:** KB2596861, KB2596810 **SharePoint Designer 2010:** KB2810069 32-bit, KB2810069 64-bit, **SharePoint Designer 2013:** KB2752096 32-bit, KB2752096 64-bit, KB2863836 32-bit, KB2863836 64-bit, KB2863854 32-bit, KB2863854 64-bit	14-022
Windows RDP Tampering vulnerability	Fixes a vulnerability which could allow an attacker to view or modify information in an active RDP session. (CVE 2014-0296)	**7:** 2965788 **8:** 2965788 **8.1:** 2965788 **2012:** 2965788 **2012 R2:** 2965788	14-030
Ancillary Function Driver (AFD) double free privilege elevation	Fixes a vulnerability which could allow elevation of privilege if an attacker with valid logon credentials is able to log on locally and run a specially crafted application. The vulnerability is triggered when the AFD improperly processes user-supplied input before passing the input to the Windows kernel. (CVE 2014-1767)	**Server 2003:** 32-bit, 64-bit **Vista:** 32-bit, 64-bit **Server 2008:** 32-bit, 64-bit **7:** 32-bit, 64-bit **Server 2008 R2:** 64-bit **8:** 32-bit, 64-bit **8.1:** 32-bit, 64-bit for systems that already have the 2919355 update (Windows 8.1 Update) installed. (See the Update	14-040

		FAQ if managing updates using Windows Server Update Services, Windows Intune, or System Center Configuration Manager.) **Server 2012:** 64-bit **Server 2012 R2:** 64-bit for systems that already have the 2919355 update (Windows 8.1 Update) installed. (See the Update FAQ if managing updates using Windows Server Update Services, Windows Intune, or System Center Configuration Manager.)	
Windows Task Scheduler Remote Elevation of Privilege	Fixes a vulnerability which could allow elevation of privilege if a user schedules a specially crafted application. (CVE 2014-4074)	**8:** 2988948 **8 (64 bit):** 2988948 **8.1:** 2988948 **8.1 (64 bit):** 2988948 **2012:** 2988948 **2012 R2:** 2988948	14-054
Vulnerabilities in Microsoft Graphics Component	Fixes two vulnerabilities by correcting the way Windows handles certain specially crafted files and by correcting the way GDI+ validates specially crafted image record types. (CVE 2014-1817 CVE 2014-1818)	**Server 2003, Vista, 2008, Windows 7, and 2008 R2:** KB2957503, KB2957509 **Windows 8, 8.1, Windows Server 2012, 2012 R2:** KB2964736, KB2964718 **Lync 2010:** KB2963285 (32-bit) KB2963285 (64-bit) **Lync 2010 Attendee:** KB2963282 (user level) (admin level) **Lync 2013:** KB2881013 (32-bit)	14-036

		KB2881013 (64-bit)	
Windows Journal Remote Code Execution	Fixes a vulnerability which could allow command execution when a user opens a specially crafted Windows Journal (.jnt) file. (CVE 2014-1824)	**Vista:** 2971850 **2008:** 2971850 **7:** 2971850 **2008 R2:** 2971850 **8:** 2971850 **8.1:** 2971850 **2012:** 2971850 **2012 R2:** 2971850	14-038
Microsoft Service Bus Denial of Service vulnerability MS14-042	Fixes a vulnerability which could allow an authenticated attacker to cause the Windows Service Bus to stop responding to AMQP messages. (CVE 2014-2814)	**2008 R2, 2012, 2012 R2:** 2972621	14-042
Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege	Resolves a vulnerability that could allow elevation of privileges if an attacker exploits a vulnerability that executes the On-Screen Keyboard (OSK) and uploads a malicious program to the intended targeted system. (CVE 2014-2781)	**Vista:** 32bit 64bit **2008:** 32bit 64bit **7:** 32bit **8:** 32bit 64bit **8.1:** 32bit 64bit **2012:** 64bit **2012 R2:** 64bit	14-039
Windows Installer EoP vulnerability	Fixes a privilege elevation vulnerability in the Windows Installer service when it improperly runs custom action scripts. To exploit this vulnerability, an attacker must first compromise a user who is logged on to the target system, then find a vulnerable `.msi` package that is installed on the target system, and then place specially crafted code on the target system that the vulnerable `.msi` package can execute. A successful attacker could gain elevated privileges on the target system, to include full administrative rights. (CVE 2015-2371)	**2003:** 32-bit, 64-bit **Vista:** 32-bit, 64-bit **7:** 32-bit, 64-bit **2008:** 32-bit, 64-bit **2008 R2:** 64-bit **8:** 32-bit, 64-bit **8.1:** 32-bit, 64-bit **2012:** 64-bit **2012 R2:** 64-bit	15-074
Windows Installer repair vulnerability	Fixes a privilege elevation vulnerability which could allow a logged-in user to run arbitrary code in kernel mode when the Windows Installer service attempts to repair a previously installed application. (CVE 2014-1814)	**2003:** 2918614 **Vista:** 2918614 **7:** 2918614 **2008:** 2918614 **2008 R2:** 2918614 **8:** 2918614 **8.1:** 2918614 **2012:** 2918614 **2012 R2:** 2918614	14-049 (superseded by MS15-074 on all vulnerable systems)
Windows LRPC ASLR bypass vulnerability	Fixes a security feature bypass vulnerability in the Local RPC (LRPC) component of Microsoft Remote Procedure Call (RPC). An LRPC server receiving a specific type of message with an unexpected data view attached, returns an error without freeing the message. This could result	KB2978668 **7:** 32-bit, 64-bit **Server 2008 R2:** 64-bit **8:** 32-bit, 64-bit **8.1:** 32-bit, 64-bit **Server 2012:** 64-bit	14-047

	in denial of service as the address space of the server fills up with these messages. Additionally, a remote attacker could use this vulnerability in conjunction with another vulnerability, such as a remote code execution vulnerability, to bypass Microsoft's Address Space Layout Randomization (ASLR) security feature and successfully exploit the second vulnerability. (CVE 2014-0316)	**Server 2012 R2:** 64-bit	
`CSyncBasePlayer` Use After Free Vulnerability	Fixes a vulnerability in Windows Media Center, which could allow command execution when a user opens a specially crafted Microsoft Office file. (CVE 2014-4060)	**Vista:** 2978742 (32-bit), 2978742 (64-bit) **Windows 7:** 2978742 (32-bit), 2978742 (64-bit) **8:** 2978742 (32-bit), 2978742 (64-bit) **8.1:** 2978742 (32-bit), 2978742 (64-bit)	14-043
Windows Media Center RCE	Fixes a vulnerability in Windows Media Center, which could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. (CVE 2015-2509)	**Vista:** 3087918 (32-bit), 3087918 (64-bit) **Windows 7:** 3087918 (32-bit), 3087918 (64-bit) **8:** 3087918 (32-bit), 3087918 (64-bit) **8.1:** 3087918 (32-bit), 3087918 (64-bit)	15-100
Kernel-Mode Drivers Vulnerabilities	Fixes three vulnerabilities, of which the most severe could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. (CVE 2014-0318 CVE 2014-1819 CVE 2014-4064)	**Server 2003:** 2993651 2993651(64), **Vista:** 2993651 2976897 2993651 (64) 2976897 (64), **Server 2008:** 2993651 2976897 2993651 (64) 2976897 (64), **Windows 7** 2993651 2976897 2993651 (64) 2976897 (64), **Windows Server 2008 R2** 2993651 2976897 **Windows 8** 2993651 2976897 2993651 (64) 2976897 (64), **Windows 8.1** 2993651 2976897	14-045

		2993651 (64) 2976897 (64), **Server 2012 and 2012 R2** 2993651 2976897 2993651 2976897	
Multiple Kernel-Mode Drivers Vulnerabilities	Fixes two vulnerabilities, of which the most severe could allow remove code execution if an attacker successfully gets someone to visit an untrusted website containing a specially crafted TrueType font. (CVE 2014-4113 CVE 2014-4148)	**Server 2003:** 3000061 3000061 (64), **Vista:** 3000061 3000061 (64), **Server 2008:** 3000061 3000061 (64), **Windows 7** 3000061 3000061 (64), **Windows Server 2008 R2** 3000061, **Windows 8** 3000061 3000061 (64), **Windows 8.1** 3000061 3000061 (64), **Server 2012** 3000061, **Server 2012 R2** 3000061	14-058
Microsoft Lync multiple vulnerabilities	Vulnerabilities in Microsoft Lync Server could allow a remote unauthenticated attacker to cause a denial of service or conduct a cross-site scripting attack. (CVE 2014-4068 CVE 2014-4070 CVE 2014-4071)	**2010:** 2982388 **2013:** 2986072, 2982389, 2992965, 2982390	14-055
Microsoft Lync TrueType font parsing vulnerability	A vulnerability in Microsoft Lync could allow remote code execution by an attacker who convinces a user to open a specially crafted document or to visit an untrusted webpage that contains embedded TrueType fonts. (CVE 2015-1671)	**2010:** 32-bit 3051464, 64-bit 3051464 **2010 Attendee:** admin-level 3051466, user-level 3051466 **2013:** 32-bit 3039779, 64-bit 3039779	15-044
Windows OLE remote code execution vulnerability	Fixes a vulnerability by modifying the way that OLE objects are activated in Windows. The vulnerability could allow remote code execution if a user opens a Microsoft Office file that contains a specially crafted OLE object. (CVE 2014-4114)	**Vista:** 3000869, 3000869 (64-bit) **Windows Server 2008:** 3000869, 3000869 (64-bit) **Windows 7:** 3000869, 3000869 (64-bit) **Windows Server 2008 R2:** 3000869 (64-bit) **Windows 8:** 3000869, 3000869	14-060

		(64-bit) **Windows 8.1:** 3000869, 3000869 (64-bit) **Windows Server 2012:** 3000869 (64-bit) **Windows Server 2012 R2:** 3000869 (64-bit)	
Microsoft Message Queuing MQAC Arbitrary Write vulnerability	Fixes a vulnerability which allows local users to take complete control of a system by sending a specially crafted IOCTL request to the Microsoft Message Queuing service. (CVE 2014-4971)	**2003:** 2993254	14-062
Microsoft FAT32 Disk Partition Driver Vulnerability	Microsoft October security update resolves an escalation in privilege in Windows FASTFAT system driver and its interaction with FAT32 disk partitions. An attacker needs local access to the system in order to successfully exploit this flaw. (CVE 2014-4115)	**Vista:** 2998579, 2998579 (64-bit) **Server 2003:** 2998579, 2998579 (64-bit) **Server 2008:** 2998579, 2998579 (64-bit)	14-063
Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution	This vulnerability could allow remote code execution if an attacker convinces a user to open a specially crafted Microsoft Word file. An attacker who successfully exploited the vulnerability would be able to run arbitrary code with the same user rights as the current user. If the current user has administrative rights, the attacker would also have administrative rights. (CVE 2014-4117)	**Microsoft SharePoint Server 2010 Service Pack 1 or 2:** 2883098	14-061
Active Directory Federation Services Information Disclosure	Fixes a vulnerability which could allow a user to gain another user's information, if the second user logs off without closing the browser. (CVE 2014-6331)	**2008:** 3003381 **2008 x64:** 3003381 **2008 R2:** 3003381 **2012:** 3003381 **2012 R2:** 3003381	14-077
SharePoint Elevation of Privilege Vulnerability	Fixes a vulnerability which could allow an authenticated attacker to run arbitrary code in the security context of the logged-on user. (CVE 2014-4116)	**Microsoft SharePoint Foundation 2010:** 2889838	14-073
SChannel vulnerability could allow Remote Code Execution	Fixes a vulnerability which could allow remote code execution when SChannel fails to properly sanitize incoming packets. (CVE 2014-6321)	**Windows Server 2003:** 2992611 2992611 (x64) **Windows Vista:** 2992611 2992611 (x64) **Windows Server 2008:** 2992611 2992611 (x64) **Windows 7:** 2992611 2992611	14-066

		(x64) **Windows Server 2008 R2:** 2992611 (x64) **Windows 8:** 2992611 2992611 (x64) **Windows 8.1:** 2992611 2992611 (x64) **Windows Server 2012:** 2992611 **Windows Server 2012 R2:** 2992611	
IIS IP and domain restriction bypass	Fixes a vulnerability which could lead to a bypass of the "IP and domain restrictions" security feature. Successful exploitation of this vulnerability could result in clients from restricted or blocked domains having access to restricted web resources. (CVE 2014-4078)	**Windows 8:** 2982998 2982998 (x64) **Windows 8.1:** 2982998 2982998 (x64) **Windows Server 2012:** 2982998 **Windows Server 2012 R2:** 2982998	14-076
Remote Desktop Protocol Failure to Audit Vulnerability	Fixes a vulnerability which could allow security feature bypass when Remote Desktop Protocol fails to properly log audit events. (CVE 2014-6318)	**Windows Vista:** 3003743 3003743 (x64) **Windows Server 2008:** 3003743 3003743 (x64) **Windows 7:** 3003743 3003743 (x64) **Windows Server 2008 R2:** 3003743 (x64) **Windows 8:** 3003743 3003743 (x64) **Windows 8.1:** 3003743 3003743 (x64) **Windows Server 2012:** 3003743 **Windows Server 2012 R2:** 3003743	14-074
Microsoft XML Core Services Remote Code Execution Vulnerability	Fixes a vulnerability which could allow remote code execution if a user opens a specially crafted webpage or file. (CVE 2014-4118)	**2003:** 2993958 **2003 (64 bit):** 2993958 **Vista** 2993958 **Vista (64 bit):** 2993958 **2008** 2993958 **2008 (64 bit):** 2993958	14-067

		Win 7 2993958 **Win 7 (64 bit):** 2993958 **2008 R2:** 2993958 **Win 8:** 2993958 **Win 8 (64 bit):** 2993958 **Win 8.1:** 2993958 **Win 8.1 (64 bit):** 2993958 **2012:** 2993958 **2012 R2:** 2993958	
Microsoft Windows Audio Service Privilege Elevation Vulnerability	Fixes a vulnerability which could allow an attacker to gain elevated privileges when used in conjunction with another vulnerability that allows remote code execution. (CVE 2014-6322)	**Vista:** 3005607 **Vista (64 bit):** 3005607 **2008:** 3005607 **2008 (64 bit):** 3005607 **Win 7:** 3005607 **Win 7 (64 bit):** 3005607 **2008 R2:** 3005607 **Win 8:** 3005607 **Win 8 (64 bit):** 3005607 **Win 8.1:** 3005607 **Win 8.1 (64 bit):** 3005607 **2012:** 3005607 **2012 R2:** 3005607	14-071
Japanese IME privilege elevation vulnerability	Resolves a privilege elevation vulnerability which could grant a malicious attacker full control of the target. (CVE 2014-4077)	**Vista:** 2992719 **Vista (64 bit):** 2992719 **2003:** 2992719 **2003 (64 bit):** 2992719 **2008:** 2992719 **2008 (64 bit):** 2992719 **Win 7:** 2992719 **Win 7 (64 bit):** 2992719 **2008 R2 (64 bit):** 2992719	14-078
Microsoft Kernel Mode Driver Vulnerability	Resolves a vulnerability that could allow an attacker to crash a target with a specially crafted TrueType font or a malicious website. (CVE 2014-6317)	**Vista:** 3002885 **Vista (64 bit):** 3002885 **2003:** 3002885 **2003 (64 bit):** 3002885 **2008:** 3002885 **2008 (64 bit):** 3002885 **Win 7:** 3002885	14-079

		Win 7 (64 bit): 3002885 **2008 R2:** 3002885 **Win 8:** 3002885 **Win 8 (64 bit):** 3002885 **Win 8.1:** 3002885 **Win 8.1 (64 bit):** 3002885 **2012:** 3002885 **2012 R2:** 3002885	
Microsoft Graphics Component Information Disclosure Vulnerability	This patch resolves a vulnerability that could allow information disclosure providing a larger attack surface. The malicious user could use this information to orchestrate other attacks. (CVE 2014-6355)	**Vista:** 3013126 **Vista (64 bit):** 3013126 **2003:** 3013126 **2003 (64 bit):** 3013126 **2008:** 3013126 **2008 (64 bit):** 3013126 **Win 7:** 3013126 **Win 7 (64 bit):** 3013126 **2008 R2:** 3013126 **Win 8:** 3013126 **Win 8 (64 bit):** 3013126 **Win 8.1:** 3013126 **Win 8.1 (64 bit):** 3013126 **2012:** 3013126 **2012 R2:** 3013126	14-085
Windows OLE Automation Array remote code execution vulnerability (MS14-064)	Fixes a Windows OLE Automation Array vulnerability that is triggered when Internet Explorer improperly accesses objects in memory. (CVE 2014-6332)	**Server 2003:** 3006226 3006226 (x64) **Vista:** 3006226 3006226 (x64) **Server 2008:** 3006226 3006226 (x64) **7:** 3006226 3006226 (x64) **Server 2008 R2:** 3006226 (x64) **8:** 3006226 3006226 (x64) **8.1:** 3006226 3006226 (x64) **Server 2012:** 3006226 (x64) **Server 2012 R2:** 3006226 (x64)	14-064
Windows OLE remote code execution vulnerability (MS14-064)	Fixes a Windows OLE vulnerability that is triggered when a user downloads, or	**Vista:** 3010788 3010788 (x64)	14-064

	receives, and then opens a specially crafted Microsoft Office file that contains OLE objects. (CVE 2014-6352)	**Server 2008:** 3010788 3010788 (x64) **7:** 3010788 3010788 (x64) **Server 2008 R2:** 3010788 (x64) **8:** 3010788 3010788 (x64) **8.1:** 3010788 3010788 (x64) **Server 2012:** 3010788 (x64) **Server 2012 R2:** 3010788 (x64)	
Microsoft SharePoint Server remote code execution vulnerability (MS15-012)	Fixes a remote code execution in Microsoft SharePoint 2010 that could allow attackers to gain the same privileges as the logged in user. (CVE 2015-0064)	**SharePoint 2010:** 2920810	15-012
Microsoft SharePoint Server remote code execution vulnerability (MS14-081)	Fixes a remote code execution in Microsoft SharePoint 2010 and 2013 that could allow attackers to gain the same privileges as the logged in user. (CVE 2014-6357)	**SharePoint 2010:** 2899581 **SharePoint 2013:** 2883050	14-081
Microsoft Application Compatibility Infrastructure Vulnerability (MS15-001)	Fixes an elevation of privilege vulnerability due to a flaw in Microsoft Windows Application Compatibility Infrastructure (`AppCompat`) in handling authorization checking of impersonation token usage. (CVE 2015-0002)	**Windows 7:** KB3023266 KB3023266 (x64) **Windows Server 2008 R2:** KB3023266 **Windows 8** KB3023266 KB3023266 (x64) **Windows 8.1** KB3023266 KB3023266 (x64) **Windows Server 2012** KB3023266 **Windows Server 2012 R2** KB3023266	15-001
Windows Kernel-Mode Driver Could Allow Remote Code Execution (MS15-010)	Fixes six vulnerabilities in Windows Kernel-Mode Driver, the most severe of which could cause an elevation of privilege. The vulnerability could be exploited if an attacker convinces a user to open a specially crafted document or visit an untrusted website that contains embedded TrueType fonts. (CVE 2015-0003, CVE 2015-0057, CVE 2015-0060, CVE 2015-0058 [Windows 8.1 and Server 2012 R2 only], CVE 2015-0059 [Windows 7, Server 2008 R2, Windows 8, Server 2012, Windows 8.1 and Server 2012 R2 only])	**Server 2003:** KB3013455 KB3013455 (x64) **Vista:** KB3013455 KB3013455 (x64) **Server 2008:** KB3013455 KB3013455 (x64) **Windows 7:** KB3013455 KB3013455 (x64) **Server 2008 R2:** KB3013455 (x64) **Windows 8:** KB3013455 KB3013455 (x64)	15-010

		Windows 8.1: KB3013455 KB3013455 (x64) **Server 2012:** KB3013455 (x64) **Server 2012 R2:** KB3013455 (x64)	
Windows Kernel-Mode Driver Could Allow Security Feature Bypass (MS15-010)	Fixes six vulnerabilities in Windows Kernel-Mode Driver, the most severe of which could cause a security feature bypass. The vulnerability could be exploited if an attacker convinces a user to open a specially crafted document or visit an untrusted website that contains embedded TrueType fonts. (CVE 2015-0010)	**Server 2003:** KB3023562 KB3023562 (x64) **Vista:** KB3023562 KB3023562 (x64) **Server 2008:** KB3023562 KB3023562 (x64) **Windows 7:** KB3023562 KB3023562 (x64) **Server 2008 R2:** KB3023562 (x64) **Windows 8:** KB3023562 KB3023562 (x64) **Windows 8.1:** KB3023562 KB3023562 (x64) **Server 2012:** KB3023562 (x64) **Server 2012 R2:** KB3023562 (x64)	15-010
Windows Kernel-Mode Driver Could Allow Remote Code Execution (MS15-023)	Fixes vulnerabilities in Windows Kernel-Mode Driver, the most severe of which could cause an elevation of privilege. The vulnerability could be exploited if an attacker convinces a user to open a specially crafted document or visit an untrusted website that contains embedded TrueType fonts. (CVE 2015-0077, CVE 2015-0094, CVE 2015-0095, CVE 2015-0078 [Windows 8, Windows 8.1, Server 2012 and Server 2012 R2 only])	**Server 2003:** 3034344 3034344 (x64) **Vista:** 3034344 3034344 (x64) **Server 2008:** 3034344 3034344 (x64) **Windows 7:** 3034344 3034344 (x64) **Server 2008 R2:** 3034344 (x64) **Windows 8:** 3034344 3034344 (x64) **Windows 8.1:** 3034344 3034344 (x64) **Server 2012:** 3034344 (x64) **Server 2012 R2:** 3034344 (x64)	15-023
Directory Traversal Elevation of Privilege in TS WebProxy fixed by MS15-004	MS15-004 resolves a vulnerability in the TS WebProxy component of Windows caused by Windows failing to properly sanitize file paths. To exploit this vulnerability, a remote attacker	**Vista:** 32-bit: KB3023299, 64-bit: KB3023299 (x64) **Win 7:**	15-004

	would first have to trick a user into downloading a specially crafted application that would exploit an existing vulnerability in Internet Explorer (IE). If the IE vulnerability were to allow remote code execution, a successful attacker could run code with the permissions of the current user. (CVE 2015-0016)	32-bit: KB3019978, KB3020387 (Remote Desktop Client 8.0), KB3020388 (Remote Desktop Client 8.1) 64-bit: KB3019978, KB3020387 (Remote Desktop Client 8.0), KB3020388 (Remote Desktop Client 8.1) **Server 2008 R2:** KB3019978, KB3020387 (Remote Desktop Client 8.0), KB3020388 (Remote Desktop Client 8.1) **Win 8:** 32-bit: KB3019978, 64-bit: KB3019978 (x64) **Win 8.1:** 32-bit: KB3019978, 64-bit: KB3019978 (x64) **Server 2012:** KB3019978 **Server 2012 R2:** KB3019978	
Microsoft Network Location Awareness Feature Bypass Vulnerability (MS15-005)	Resolves a vulnerability that could allow a malicious user to bypass the security of the intended target by altering the firewall policy and/or configuration of certain services. (CVE 2015-0006)	**Vista:** KB3022777 KB3022777 (x64) **Win 7:** KB3022777 KB3022777 (x64) **Win 2008:** KB3022777 KB3022777 (x64) **Win 2008 R2:** KB3022777 (x64) **Win 8:** KB3022777 KB3022777 (x64) **Win 8.1:** KB3022777 KB3022777 (x64) **2012:** KB3022777 **2012 R2:** KB3022777	15-005
Windows Error Reporting Security Feature Bypass Vulnerability	Fixes a security feature bypass vulnerability in Windows Error	**Windows 8:** KB3004365	15-006

(MS15-006)	Reporting (WER) by correcting how WER interacts with processes. (CVE 2015-0001)	KB3004365 (x64) **Windows 8.1** KB3004365 KB3004365 (x64) **Windows Server 2012** KB3004365 **Windows Server 2012 R2** KB3004365	
Netlogon and Kerberos Elevation of Privilege Vulnerability (MS16-101)	Fixes privilege elevation vulnerabilities in netlogon and kerberos services. A successful attack would elevate the privileges of an attacker on the workstation. (CVE 2016-3237 CVE 2016-3300)	**Windows Vista**: KB3167679, KB3167679 (64-bit) **Windows 2008**: KB3167679, KB3167679 (64-bit) **Windows 7**: KB3167679, KB3167679 (64-bit) **Windows 2008 R2**: KB3167679 **Windows 8.1**: KB3167679, KB3167679 (64-bit) **Windows 2012**: KB3177108 **Windows 2012 R2**: KB3177108, KB3167679 **Windows 10**: KB3176492, KB3176492 (64-bit) **Windows 10 (Build 1511)**: KB3176493, KB3176493 (64-bit) **Windows 10 (Build 1607)**: KB3176495, KB3176495 (64-bit)	16-101
Network Policy Server RADIUS Implementation could cause Denial of Service (MS16-021)	Fixes a vulnerability which could prevent RADIUS authentication on the Network Policy Server (NPS) if an attacker sends specially crafted username strings. (CVE 2016-0050)	**2008:** KB3133043 KB3133043 (x64) **2008 R2:** KB3133043 **Windows Server 2012** KB3133043 **Windows Server 2012 R2** KB3133043	16-021
Network Policy Server RADIUS Implementation could cause Denial of Service (MS15-007)	Fixes a vulnerability which could prevent RADIUS authentication on the Internet Authentication Service (IAS)	**2003:** KB3014029 KB3014029 (x64) **2008:** KB3014029	15-007

	or Network Policy Server (NPS), if an attacker sends specially crafted username strings. (CVE 2015-0015)	KB3014029 (x64) **2008 R2:** KB3014029 **Windows Server 2012** KB3014029 **Windows Server 2012 R2** KB3014029	
WebDAV kernel-mode driver impersonation-level security bypass	Fixes a vulnerability which could allow an attacker to gain elevated privileges allowing them to intercept WebDAV requests for files from any server and redirect them to return malicious files. (CVE 2015-0011)	**2003:** 3019215 **Vista:** 3019215 **2008:** 3019215 **7:** 3019215 **2008 R2:** 3019215 **8:** 3019215 **8.1:** 3019215 **2012:** 3019215 **2012 R2:** 3019215	15-008
WebDAV security bypass allows information disclosure	Fixes a vulnerability which could allow information disclosure if an attacker forces an encrypted Secure Socket Layer (SSL) 2.0 session with a WebDAV server that has SSL 2.0 enabled and uses a man-in-the-middle (MiTM) attack to decrypt portions of the encrypted traffic. (CVE 2015-2476)	**Vista:** 3076949 32-bit, 3076949 64-bit **2008:** 3076949 32-bit, 3076949 64-bit **7:** 3076949 32-bit, 3076949 64-bit **2008 R2:** 3076949 **8:** 3076949 32-bit, 3076949 **8.1:** 3076949 32-bit, 3076949 64-bit **2012:** 3076949 **2012 R2:** 3076949	15-089
Windows User Profile Service Privilege Elevation Vulnerability (MS15-003)	Fixes a vulnerability which could allow an attacker to gain elevated privileges due to a flaw in the Windows User Profile Service. (CVE 2015-0004)	**2003:** 3021674 3021674 (64-bit) **Vista:** 3021674 3021674 (64-bit) **7:** 3021674 3021674 (64-bit) **2008:** 3021674 3021674 (64-bit) **2008 R2:** 3021674 (64-bit) **8:** 3021674 3021674 (64-bit) **8.1:** 3021674 3021674 (64-bit) **2012:** 3021674 **2012 R2:** 3021674	15-003
Group Policy Code Execution Vulnerability (MS15-011)	Fixes a code execution vulnerability that can be triggered when a user connects to a rogue network with a domain configured. (CVE 2015-0008)	**Vista:** KB3000483 KB3000483 (x64) **Windows Server 2008:** KB3000483	15-011

		KB3000483 (x64) **Windows 7:** KB3000483 KB3000483 (x64) **Windows Server 2008 R2:** KB3000483 **Windows 8** KB3000483 KB3000483 (x64) **Windows 8.1** KB3000483 KB3000483 (x64) **Windows Server 2012** KB3000483 **Windows Server 2012 R2** KB3000483	
Windows Create Process Elevation of Privilege Vulnerability (MS15-015)	Fixes an elevation of privilege vulnerability because the application fails to properly validate and enforce impersonation levels. An attacker could bypass impersonation-level security checks and gain elevated privileges on a targeted system. (CVE 2015-0062)	**Windows 7:** KB3031432 KB3031432 (x64) **Windows Server 2008 R2:** KB3031432 **Windows 8** KB3031432 KB3031432 (x64) **Windows 8.1** KB3031432 KB3031432 (x64) **Windows Server 2012** KB3031432 **Windows Server 2012 R2** KB3031432	15-015
Group Policy security feature bypass vulnerability	Fixes a vulnerability that could allow a man-in-the-middle attacker to cause Group Policy settings to revert to their default, and potentially less secure, state by modifying domain controller responses to client requests. (CVE 2015-0009)	**2003:** 3004361 **Vista:** 3004361 **2008:** 3004361 **7:** 3004361 **2008 R2:** 3004361 **8:** 3004361 **8.1:** 3004361 **2012:** 3004361 **2012 R2:** 3004361	15-014
Microsoft Graphics Component Information Disclosure Vulnerability (MS15-016)	Fixes a vulnerability in the Microsoft graphics component that could allow information gathering. This vulnerability exists due to the improper handling of specially crafted `TIFF` files. (CVE 2015-0061)	**2003:** 3029944 3029944 (64-bit) **Vista:** 3029944 3029944 (64-bit) **2008:** 3029944 3029944 (64-bit) **2008 R2** 3029944 **7:** 3029944 3029944 (64-bit) **8:** 3029944 3029944 (64-bit) **8.1:** 3029944	15-016

		3029944 (64-bit) **2012:** 3029944 **2012 R2:** 3029944	
Microsoft Windows RDP Free Failure Denial of Service	Fixes a vulnerability that could allow a remote attacker to consume resources by sending multiple invalid RDP connection requests. (CVE 2015-0079)	**Windows 7:** KB3035017 KB3035017 (x64) and KB3036493 KB3036493 (x64) **Windows 8** KB3035017 KB3035017 (x64) **Windows 8.1** KB3035017 KB3035017 (x64) **Windows Server 2012** KB3035017 **Windows Server 2012 R2** KB3035017	15-030
Windows Text Services Remote Code Execution vulnerability	Fixes a vulnerability in Windows Text Services which could allow command execution when a user browses to a specially crafted website or opens a specially crafted file. (CVE 2015-0081)	**2003:** 3033889 **Vista:** 3033889 **2008:** 3033889 **2008 R2:** 3033889 **7:** 3033889 **8:** 3033889 **8.1:** 3033889 **2012:** 3033889 **2012 R2:** 3033889	15-020
DLL Planting Remote Code Execution vulnerability	Fixes a vulnerability in the loading of DLL files which could allow command execution when a user opens a file contained in the same directory as a specially crafted DLL. (CVE 2015-0096)	**2003:** 3039066 **Vista:** 3039066 **2008:** 3039066 **2008 R2:** 3039066 **7:** 3039066 **8:** 3039066 **8.1:** 3039066 **2012:** 3039066 **2012 R2:** 3039066	15-020
Windows Photo Decoder Component Information Disclosure (MS15-029)	Fixes a vulnerability in Microsoft Windows which could could allow information disclosure if a user browses to a website containing a specially crafted JPEG XR (.JXR) image. (CVE 2015-0076)	**Vista:** 3035126 3035126 (x64) **2008:** 3035126 3035126 (x64) **2008 R2:** 3035126 (x64) **7:** 3035126 3035126 (x64) **8:** 3035126 3035126 (x64) **8.1:** 3035126 3035126 (x64) **2012:** 3035126 (x64) **2012 R2:** 3035126 (x64)	15-029

NETLOGON Spoofing vulnerability	Fixes a vulnerability in the Netlogon service which could allow an attacker who is already logged into a computer in the domain to obtain information for the secure channel of another computer. (CVE 2015-0005)	**2003:** 3002657 **2008:** 3002657 **2008 R2:** 3002657 **2012:** 3002657 **2012 R2:** 3002657	15-027
Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (MS15-019)	Fixes a remote code execution vulnerability that if exploited could allow a malicious attacker to gain the same user rights as the current logged in user and possibly complete control of the system. (CVE 2015-0032)	Apply the appropriate patch or patches referenced in Microsoft Security Bulletin MS15-019.	15-019
Multiple vulnerabilities in Adobe Font Driver (MS15-021)	Fixes eight vulnerabilities where the most severe could allow remote code execution. These vulnerabilities exist because of the flaw in the way how the font parser allocates memory and how objects in memory are handled. (CVE 2015-0074 CVE 2015-0087 CVE 2015-0088 CVE 2015-0089 CVE 2015-0090 CVE 2015-0091 CVE 2015-0092 CVE 2015-0093)	**2003** KB3032323 KB3032323 (64-bit) **Vista** KB3032323 KB3032323 (64-bit) **2008** KB3032323 KB3032323 (64-bit) **7** KB3032323 KB3032323 (64-bit) **2008 R2** KB3032323 **8** KB3032323 KB3032323 (64-bit) **8.1** KB3032323 KB3032323 (64-bit) **2012** KB3032323 **2012 R2** KB3032323	15-021
Vulnerability in PNG Processing Could Allow Information Disclosure (MS15-024)	This update resolves a vulnerability that could allow an attacker to obtain sensitive data if the victim is convinced to visit the malicious website. (CVE 2015-0080)	**2003** KB3035132 KB3035132 (64-bit) **Vista** KB3035132 KB3035132 (64-bit) **2008** KB3035132 KB3035132 (64-bit) **7** KB3035132 KB3035132 (64-bit) **2008 R2** KB3035132 **8** KB3035132 KB3035132 (64-bit) **8.1** KB3035132 KB3035132 (64-bit) **2012** KB3035132	15-024

		2012 R2 KB3035132	
Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (MS15-025)	Fixes two vulnerabilities in the Windows Kernel that could allow elevation of privilege. One vulnerability exists due to a flaw in Windows Registry Virtualization and the other due to improper enforcement of impersonation levels. (CVE 2015-0073 CVE 2015-0075)	**Server 2003:** 3033395 3033395 (64-bit) **Vista:** 3035131 3035131 (64-bit) **Server 2008:** 3035131 3035131 (64-bit) **Windows 7:** 3035131 3035131 (64-bit) **Server 2008 R2:** 3035131 **Windows 8:** 3035131 3035131 (64-bit) **Windows 8.1:** 3035131 3035131 (64-bit) **Server 2012:** 3035131 **Server 2012 R2:** 3035131	15-025
NtCreateTransactionManager Type Confusion elevation of privilege vulnerability (MS15-038)	Microsoft Windows contains a type confusion flaw related to NtCreateTransactionManager that may result in the operating system failing to properly validate and enforce impersonation levels. This may allow a local attacker to gain elevated privileges. (CVE 2015-1643)	**Vista:** 3045685 3045685 (64-bit) **Server 2008:** 3045685 3045685 (64-bit) **Windows 7:** 3045685 3045685 (64-bit) **Server 2008 R2:** 3045685 **Windows 8:** 3045685 3045685 (64-bit) **Windows 8.1:** 3045685 3045685 (64-bit) **Server 2012:** 3045685 **Server 2012 R2:** 3045685	15-038
Windows MS-DOS device name elevation of privilege vulnerability (MS15-038)	Microsoft Windows contains a flaw that is due to the operating system failing to properly validate and enforce impersonation levels when handling an MS-DOS device name. This may allow a local attacker to gain elevated privileges. (CVE 2015-1644)	**Vista:** 3045999 3045999 (64-bit) **Server 2008:** 3045999 3045999 (64-bit) **Windows 7:** 3045999 3045999 (64-bit) **Server 2008 R2:** 3045999 **Windows 8:** 3045999 3045999 (64-bit)	15-038

		Windows 8.1: 3045999 3045999 (64-bit) **Server 2012:** 3045999 **Server 2012 R2:** 3045999	
Task Scheduler Feature Bypass Vulnerability (MS15-028)	A vulnerability in Windows Task Scheduler due to improper validation of impersonation levels. A successful attack could allow a security bypass. (CVE 2015-0084)	**Windows 7:** 3030377 3030377 (64-bit) **Server 2008 R2:** 3030377 **Windows 8:** 3030377 3030377 (64-bit) **Windows 8.1:** 3030377 3030377 (64-bit) **Server 2012:** 3030377 **Server 2012 R2:** 3030377	15-028
Microsoft Graphics Component Remote Code Execution Vulnerability (MS15-035)	MS15-035 fixes a remote code execution vulnerability that exists due to Microsoft Windows improperly handling specially crafted enhanced metafile (EMF) files. (CVE 2015-1645)	**Windows Server 2003:** 3046306 3046306 (64-bit) **Windows Vista:** 3046306 3046306 (64-bit) **Windows Server 2008:** 3046306 3046306 (64-bit) **Windows 7:** 3046306 3046306 (64-bit) **Windows Server 2008 R2:** 3046306	15-035
Windows Hyper-V Denial of Service (MS15-042)	MS15-042 fixes a denial of service vulnerability in Windows Hyper-V. An attacker must be authenticated and run a specially crafted application in a VM session to exploit this. (CVE 2015-1647)	**Windows 8.1:** 3047234 (64-bit) **Windows Server 2012 R2:** 3047234	15-042
Two Hyper-V Privileged Guest Remote Code Execution vulnerabilities	MS15-068 fixes two vulnerabilities in Windows Hyper-V that could result in remote code execution on the system hosting the Hyper-V server. The first is a buffer overflow vulnerability caused by the way Hyper-V handles packet size memory initialization. The second is due to the way Hyper-V initializes system data structures in guest virtual machines. To exploit these vulnerabilities, an attacker must be an authenticated, privileged user on the guest virtual machine, and then run a specially crafted application. (CVE 2015-2361, CVE 2015-2362)	**Windows Server 2008:** KB3046339 (64-bit) **Windows Server 2008 R2:** KB3046339 (64-bit) **Windows 8:** KB3046339 (64-bit) **Windows 8.1:** KB3046339 (64-bit), KB3046359 (64-bit)	15-068

		Windows Server 2012: KB3046339 **Windows Server 2012 R2:** KB3046339, KB3046359	
Windows Hyper-V Security Feature Bypass (MS15-105)	MS15-105 fixes a security feature bypass vulnerability in Windows Hyper-V. An attacker who runs a specially crafted application could cause Windows Hyper-V to incorrectly apply access control list configuration settings. (CVE 2015-2534)	**Windows 8.1:** 3087088 (64-bit) **Windows Server 2012 R2:** 3087088 **Windows 10:** 3081455 (64-bit)	15-105
Windows Hyper-V Susceptibility (MS16-045)	MS16-045 fixes vulnerabilities in Windows Hyper-V. The most severe of the vulnerabilities could allow remote code execution if an authenticated attacker on a guest operating system runs a specially crafted application that causes the Hyper-V host operating system to execute arbitrary code. Customers who have not enabled the Hyper-V role are not affected. (CVE 2016-0088 CVE 2016-0089 CVE 2016-0090)	**Windows 8.1:** 3135456 (64-bit) **Windows Server 2012:** 3135456 **Windows Server 2012 R2:** 3135456 **Windows 10:** 3147461 (64-bit)	16-045
Microsoft SharePoint Server Word Automation vulnerabilities	The Microsoft SharePoint Server Word Automation service is affected by a memory corruption vulnerability and two use-after-free vulnerabilities which could allow code execution when a user opens a specially crafted file. (CVE 2015-1641 CVE 2015-1649 CVE 2015-1650)	**SharePoint Server 2010:** 2553164 **SharePoint Server 2013:** 2965215	15-033
Active Directory Federation Services (AD FS) information disclosure	Fixes a vulnerability where Active Directory Federation Services (AD FS) fails to properly log off a user which could allow information disclosure when a user leaves the browser open after logging off from an application. (CVE 2015-1638)	**Windows Server 2012 R2:** 3045711	15-040
Microsoft XML Core Services Security Feature Bypass Vulnerability	This security update resolves a vulnerability in Microsoft Windows that addresses a vulnerability that could allow an attacker to bypass a security feature if a user clicks a specially crafted link. (CVE 2015-1646)	**Vista:** 3046482 3046482 (64-bit) **Server 2003:** 3046482 3046482 (64-bit) **Windows 7:** 3046482 3046482 (64-bit) **Server 2008:** 3046482 3046482 (64-bit) **Server 2008 R2:** 3046482	15-039
Microsoft XML Core Services Information Disclosure Vulnerabilities	This security update resolves three vulnerabilities in Microsoft Windows that could allow an attacker to disclose information if a user clicks a specially crafted link.	**Vista:** 3076895 3076895 (64-bit) **Windows 7:** 3076895 3076895 (64-bit)	15-084

	CVE-2015-2434 and CVE-2015-2471 do not apply to XML Core Services 6.0. All three CVEs apply to XML Core Services 3.0. (CVE 2015-2434 [ver 3.0 only] CVE 2015-2440 CVE 2015-2471 [ver 3.0 only])	**Server 2008:** 3076895 3076895 (64-bit) **Server 2008 R2:** 3076895 (64-bit) **Windows 8:** 3076895 3076895 (64-bit) **Windows 8.1:** 3076895 3076895 (64-bit) **Server 2012:** 3076895 (64-bit) **Server 2012 R2:** 3076895 (64-bit)	
Microsoft SharePoint Server remote code execution	This security update resolves a vulnerability in Microsoft SharePoint Server 2007, 2010, and 2013 that could allow remote code execution. This vulnerability exists due to improper sanitization of specially crafted pages. (CVE 2015-1700)	**SharePoint 2007:** 2760412 2760412 (64-bit) **SharePoint 2010:** 3017815 (Foundation Server) 2956192 (Business Productivity Server) **SharePoint 2013:** 3054792	15-047
Windows Journal command execution vulnerabilities	Fixes multiple vulnerabilities which could allow command execution when a user opens a specially crafted Journal file. (CVE 2015-1675 CVE 2015-1695 CVE 2015-1696 CVE 2015-1697 CVE 2015-1698 CVE 2015-1699)	**Vista:** 3046002 **2008:** 3046002 **7:** 3046002 **2008 R2:** 3046002 **8:** 3046002 **8.1:** 3046002 **2012:** 3046002 **2012 R2:** 3046002	15-045
Microsoft Management Console File Format Denial of Service	Fixes a vulnerability which could cause a denial of service when a user opens a specially crafted `.msc` file. (CVE 2015-1681)	**Vista:** 3051768 **2008:** 3051768 **7:** 3051768 **2008 R2:** 3051768 **8:** 3051768 **8.1:** 3051768 **2012:** 3051768 **2012 R2:** 3051768	15-054
Windows Kernel Security Feature Bypass Vulnerability (MS15-052)	Resolves a vulnerability by correcting Windows Kernel validation origins of request. A malicious user could exploit this vulnerability using security feature bypass if run using a specially crafted application. (CVE 2015-1674)	**8:** 3050514 3050514 (64-bit) **8.1:** 3050514 3050514 (64-bit) **2012:** 3050514 **2012 R2:** 3050514	15-052
Schannel 512-bit DHE key vulnerability	Increases the minimum allowable Diffie-Hellman ephemeral key length to 1024 bits to prevent various attacks which could allow information	**2003:** 3061518 **Vista:** 3061518 **2008:** 3061518 **7:** 3061518	15-055

	disclosure during encrypted TLS sessions. (CVE 2015-1716)	**2008 R2:** 3061518 **8:** 3061518 **8.1:** 3061518 **2012:** 3061518 **2012 R2:** 3061518	
Microsoft SharePoint and WebApps memory corruption vulnerability	MS15-046 resolves a memory corruption vulnerability in Microsoft SharePoint Server 2010, Microsoft SharePoint Server 2013, Microsoft Office WebApps 2010, and Microsoft Office WebApps 2013 that could be used to execute remote code if a user opens a specially crafted file. (CVE 2015-1682)	**SharePoint 2010:** 3017815 (Foundation Server) 2965233 (Word automation services) 2956194 (Excel services) **Office Web Apps 2010:** 2956140 2956193 (Excel web app) **SharePoint 2013:** 3039736 (Enterprise Server) 3023055 (Word automation server) 3039725 (Excel services) **Office Web Apps 2013:** 3039748	15-046
Microsoft SharePoint and Office Web Apps remote code execution	MS16-148 resolves information disclosure vulnerabilities in Microsoft SharePoint Server 2010, Excel and Word Automation Services, and Office Web Apps, in which information is leaked that could aid an attacker in performing additional attacks. (CVE 2016-7265 CVE 2016-7268 CVE 2016-7290 CVE 2016-7291)	**SharePoint 2007 (32 bit):** 3127892 **SharePoint 2007 (32 bit):** 3127892 **Office Web Apps 2010:** 3128035 **Excel Services on SharePoint Server 2010:** 3128029 **Word Automation on SharePoint Server 2010:** 3128026	16-148
Microsoft SharePoint and Office Web Apps remote code execution	MS16-121 resolves a remote code execution vulnerability in Microsoft SharePoint Server 2010, Microsoft SharePoint Server 2013, Microsoft Office WebApps 2010, Microsoft Office WebApps 2013, and Office Online that could be used to execute remote code if a user opens a specially crafted file. (CVE 2016-7193)	**SharePoint 2010:** 3118377 **Office Web Apps 2010:** 3118384 **SharePoint 2013:** 3118352 **Office Web Apps 2013:** 3118360 **Office Online:** 3127897	16-121
Service Control Manager Elevation of Privilege Vulnerability	Fixes a vulnerability where Windows Service Control Manager (SCM) improperly verifies impersonation levels. (CVE 2015-1702)	**Vista:** KB3055642 KB3055642 (64-bit) **2008:** KB3055642 KB3055642 (64-bit) **7:** KB3055642	15-050

		KB3055642 (64-bit) **2008 R2:** KB3055642 (64-bit) **8:** KB3055642 KB3055642 (64-bit) **8.1:** KB3055642 KB3055642 (64-bit) **2012:** KB3055642 **2012 R2:** KB3055642	
VBScript and JScript ASLR Bypass Vulnerabilities.	MS15-053 fixes two vulnerabilities when JScript and VBScript engines fail to use the Address Space Layout Randomization (ASLR) security feature. (CVE 2015-1684 CVE 2015-1686)	**2003/Vista:** JScript 5.6 and VBScript 5.6 JScript 5.7 and VBScript 5.7 **2008:** JScript 5.8 and VBScript 5.8	15-053
Microsoft Font Drivers Vulnerabilities and Win32k Elevation of Privilege Vulnerability	Resolves several vulnerabilities by correcting how the Windows DirectWrite library interacts with OpenType or TrueType fonts. It also fixes how the kernel-mode driver handles objects in memory. (CVE 2015-1670, CVE 2015-1671, CVE 2015-1676, CVE 2015-1677, CVE 2015-1678, CVE 2015-1679, CVE 2015-1680, CVE 2015-1701)	**Vista:** 3045171 3045171 (64-bit) **7:** 3045171 3045171 (64-bit) **8:** 3045171 3045171 (64-bit) **8.1:** 3045171 3045171 (64-bit) **2003:** 3045171 3045171 (64-bit) **2008:** 3045171 3045171 (64-bit) **2008 R2:** 3045171 (64-bit) **2012:** 3045171 **2012 R2:** 3045171	15-044 15-051
Microsoft Common Control use after free vulnerability	Fixes a vulnerability which could allow command execution when a user clicks on a link to specially crafted content and then invokes the F12 Developer Tools in Internet Explorer. (CVE 2015-1756)	**Vista:** 3059317 **2008:** 3059317 **7:** 3059317 **2008 R2:** 3059317 **8:** 3059317 **8.1:** 3059317 **2012:** 3059317 **2012 R2:** 3059317	15-060
Windows kernel-mode drivers privilege elevation	Fixes multiple vulnerabilities which could allow a logged-on user to gain elevated privileges. (CVE 2015-1719 CVE 2015-1720 CVE 2015-1721 CVE 2015-1722 CVE 2015-1723 CVE 2015-1724 CVE 2015-1725 CVE 2015-1726 CVE 2015-1727 CVE 2015-1768 CVE 2015-2360)	**2003**: 3057839 **Vista**: 3057839 **2008**: 3057839 **7**: 3057839 **2008 R2**: 3057839 **8**: 3057839 **8.1**: 3057839 **2012**: 3057839 **2012 R2**: 3057839	15-061

Windows Media Player Remote Code Execution Vulnerability (MS15-057)	Fixes a vulnerability in Windows Media Player that could allow an attacker to take complete control of a system. This vulnerability exists due to improper handling of specially crafted `DataObjects`. (CVE 2015-1728)	**2003:** 3033890 3033890 (64-bit) **Vista:** 3033890 3033890 (64-bit) **2008:** 3033890 3033890 (64-bit) **7:** 3033890 3033890 (64-bit) **2008 R2:** 3033890	15-057
Active Directory Federation Services Elevation of Privilege	Fixes a vulnerability which could allow elevation of privilege if an attacker submits a specially crafted URL to the target. (CVE 2015-1757)	**2008:** 3062577 **2008 x64:** 3062577 **2008 R2:** 3062577 **2012:** 3062577	15-062
Windows Remote Code Execution Vulnerabilities	This fix resolves vulnerabilities in Microsoft Windows that could allow remote code execution by placing a specially crafted dynamic link library (DLL) file in the target user's current working directory. This ultimately grants complete control of an affected system. (CVE 2015-2368 CVE 2015-2369)	**2003:** 3067903 3067903 (64-bit) **Vista:** 3067903 3067903 (64-bit) **2008:** 3067903 3067903 **7:** 3067903 3070738 3067903 (64-bit) 3070738 (64-bit) **2008 R2:** 3067903 3070738 (64-bit) **8.1:** 3061512 3061512(64-bit) **2012 R2:** 3067903	15-069
Windows OLE Elevation Of Privilege Vulnerabilities	This update resolves vulnerabilities in Microsoft Windows that could allow elevation of privilege. (CVE 2015-2416 CVE 2015-2417)	**2003:** 3072633 3072633 (64-bit) **Vista:** 3072633 3072633 (64-bit) **2008:** 3072633 3072633 (64-bit) **7:** 3072633 3072633 (64-bit) **2008 R2:** 3072633 (64-bit) **8:** 3072633 3072633 (64-bit) **8.1:** 3072633 3072633 (64-bit) **2012:** 3072633 **2012 R2:** 3072633	15-075
Windows LoadLibrary Elevation of Privilege Vulnerability	Fixes an elevation of privilege vulnerability in the Windows Kernel. The vulnerability exists in Microsoft Windows LoadLibrary because it fails to properly validate user input. An authenticated attacker could place a **`.dll`** file in a local directory on the machine or on a network share. If the	**Vista:** 3063858 3063858 (64-bit) **2008:** 3063858 3063858 (64-bit) **7:** 3063858 3063858 (64-bit) **2008 R2:** 3063858	15-063

	attacker successfully entices a user to run a specially crafted application that loads the malicious `.dll` file, the attacker could gain full administrative rights. (CVE 2015-1758)	**8:** 3063858 3063858 (64-bit) **2012:** 3063858	
Vulnerability in RDP Could Allow Remote Code Execution	A vulnerability in Microsoft Windows could allow remote code execution if an attacker sends a specially crafted sequence of packets to a targeted system with the Remote Desktop Protocol (RDP) server service enabled. (CVE 2015-2373)	**7:** 3067904 3067904 (64-bit) **8:** 3067904 3067904 (64-bit) **2012:** 3067904	15-067
Windows RPC privilege elevation	Fixes a vulnerability which could allow a logged-in user to take full control of the system. (CVE 2015-2370)	**2003**: 3067505 **2003 R2**: 3067505 **Vista**: 3067505 **2008**: 3067505 **7**: 3067505 **2008 R2**: 3067505 **8**: 3067505 **8.1**: 3067505 **2012**: 3067505 **2012 R2**: 3067505	15-076
Windows Graphic Component Elevation of Privilege Vulnerability (MS15-072)	Fixes a vulnerability which could allow privilege elevation due to improper processing of bitmap conversions. (CVE 2015-2364)	**2003:** 3069392 3069392 (64=bit) **Vista:** 3069392 3069392 (64-bit) **2008:** 3069392 3069392 (64-bit) **7:** 3069392 3069392 (64-bit) **2008 R2:** 3069392 **8:** 3069392 3069392 (64-bit) **8.1:** 3069392 3069392 (64-bit) **2012:** 3069392 **2012 R2:** 3069392	15-072
VBScript Memory Corruption Vulnerability (MS15-066)	Fixes a vulnerability which could allow remote code execution if a user visits a specially crafted website. (CVE 2015-2372)	Apply the patch.	15-066
Windows kernel-mode drivers privilege elevation	Fixes multiple vulnerabilities which could allow a logged-on user to gain elevated privileges. (CVE 2015-2363 CVE 2015-2365 CVE 2015-2366 CVE 2015-2367 CVE 2015-2381 CVE 2015-2382)	**2003**: 3070102 3070102 (64-bit) **Vista**: 3070102 3070102 (64-bit) **2008**: 3070102 3070102 (64-bit) **7**: 3070102 3070102 (64-bit) **2008 R2**: 3070102 **8**: 3070102 3070102 (64-bit) **8.1**: 3070102 3070102 (64-bit) **2012**: 3070102 **2012 R2**: 3070102	15-073

Windows kernel memory Elevation of Privilege Vulnerability	Resolves Vulnerabilities in Windows that can allow privileged elevation if an attacker runs a specially crafted application in a system. This Vulnerabilities exist due to the way the Windows Kernel handles objects in Memory. An attacker would first have to log on to the system to exploit the vulnerabilities. (CVE 2015-6171 CVE 2015-6173 CVE 2015-6174 CVE 2015-6175)	**Vista**: 3109094 (32-bit) 3109094 (64-bit) **2008**: 3109094 (32-bit) 3109094 (64-bit) **7**: 3109094 (32-bit) 3109094 (64-bit) **2008 R2**: 3109094 **8**: 3109094 (32-bit) 3109094 (64-bit) **8.1**: 3109094 (32-bit) 3109094 (64-bit) **2012**: 3109094 **2012 R2**: 3109094 **10**: 3116869 (32-bit) 3116869 (64-bit) **10 v1511**: 3116900 (32-bit) 3116900 (64-bit)	15-135
NETLOGON Elevation of Privilege Vulnerability (MS15-071)	Fixes a vulnerability which could allow elevation of privilege if an attacker with access to a primary domain controller (PDC) on a target network runs a specially crafted application to establish a secure channel to the PDC as a backup domain controller (BDC). (CVE 2015-2374)	**2003:** 3068457 **2008:** 3068457 3068457(64-bit) **2008 R2:** 3068457 **2012:** 3068457 **2012 R2:** 3068457	15-071
Microsoft SharePoint vulnerabilities	Fixes two vulnerabilities in Excel Services on SharePoint Server 2007, 2010, and 2013 which could allow memory corruption or ASLR bypass. (CVE 2015-2375 CVE 2015-2376)	**SharePoint 2007:** 2837612 **SharePoint 2010:** 3054968 **SharePoint 2013:** 3054861	15-070
Windows Adobe font driver elevation of privilege vulnerability (MS15-077)	This update resolves an elevation of privilege vulnerability which exists in Adobe Type Manager Font Driver (ATMFD) when it fails to properly handle objects in memory. (CVE 2015-2387)	**2003** 3077657 3077657 (64-bit) **Vista** 3077657 3077657 (64-bit) **2008** 3077657 3077657 (64-bit) **7** 3077657 3077657 (64-bit) **2008 R2** 3077657 **8** 3077657 3077657 (64-bit) **8.1** 3077657 3077657 (64-bit) **2012** 3077657 **2012 R2** 3077657	15-077
Windows OpenType Font Driver Vulnerability (MS15-078)	This update resolves a remote code execution vulnerability when Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts. (CVE 2015-2426)	**Vista** 3079904 3079904 (64-bit) **2008** 3079904 3079904 (64-bit) **7** 3079904 3079904 (64-bit)	15-078

		2008 R2 3079904 **8** 3079904 3079904 (64-bit) **8.1** 3079904 3079904 (64-bit) **2012** 3079904 **2012 R2** 3079904	
Windows Object Manager symbolic link sandbox escape	Fixes multiple vulnerabilities which could allow a logged-on user to gain elevated privileges. (CVE 2015-2428 CVE 2015-2429 CVE 2015-2430)	**Vista:** 3060716 **2008:** 3060716 **7:** 3060716 **2008 R2:** 3060716 **8:** 3060716 **8.1:** 3060716 **2012:** 3060716 **2012 R2:** 3060716	15-090
Server Message Block Memory Corruption Vulnerability	Fixes a memory corruption vulnerability in SMB Advanced Error Handling vulnerabilities which could allow remote code execution if an attacker sends a specially crafted string to the SMB server error logging. (CVE 2015-2474)	**Vista:** 3073921 **2008:** 3073921	15-083
Windows Journal remote code execution vulnerability (MS15-098)	Fixes a remote code execution vulnerability that exists in Windows Journal due to improper handling of specially crafted journal files. (CVE 2015-2513 CVE 2015-2514 CVE 2015-2516 CVE 2015-2519 CVE 2015-2530)	**Vista**: 3069114 3069114 (64-bit) **2008**: 3069114 3069114 (64-bit) **7**: 3069114 3069114 (64-bit) **2008 R2**: 3069114 **8**: 3069114 3069114 (64-bit) **8.1**: 3069114 3069114 (64-bit) **2012**: 3069114 **2012 R2**: 3069114 **10**: 3081455 3081455 (64-bit)	15-098
Windows Journal remote code execution vulnerability (MS15-114)	Addresses a remote code execution vulnerability that modifies how Windows Journal parses Journal files. (CVE 2015-6097)	**Vista**: 3100213 3100213 (64-bit) **2008**: 3100213 3100213 (64-bit) **7**: 3100213 3100213 (64-bit) **2008 R2**: 3100213	15-114
Microsoft Graphics Component vulnerabilities	Fixes multiple vulnerabilities, the most critical of which could allow command execution when a user opens a document containing embedded TrueType or OpenType fonts. (CVE 2015-2432 CVE 2015-2433 CVE 2015-2435 CVE 2015-2453 CVE 2015-2454 CVE 2015-2455 CVE 2015-2456 CVE 2015-2458 CVE 2015-2459 CVE 2015-2460 CVE 2015-2461 CVE 2015-2462 CVE 2015-2463 CVE 2015-2464 CVE	**Vista**: 3078601 **2008**: 3078601 **7**: 3078601 **2008 R2**: 3078601 **8**: 3078601 **8.1**: 3078601 **2012**: 3078601 **2012 R2**: 3078601	15-080

	2015-2465)		
Mount Manager Elevation of Privilege Vulnerability (MS15-085)	A vulnerability in Windows Mount Manager exists due to improper handling of certain symbolic links. A successful exploit could give the attacker elevated privileges. (CVE 2015-1769)	**Vista**: 3071756 3071756 (64-bit) **2008**: 3071756 3071756 (64-bit) **7**: 3071756 3071756 (64-bit) **2008R2**: 3071756 **8**: 3071756 3071756 (64-bit) **8.1**: 3071756 3071756 (64-bit) **2012**: 3071756 **2012R2**: 3071756 **10**: 3081436 3081436 (64-bit)	15-085
UDDI Services XSS allows Elevation of Privilege (MS15-087)	Fixes a vulnerability which could allow information disclosure including authorization tokens due to a failure when sanitizing the search parameter. (CVE 2015-2475)	**2008**: 32-bit (3073893) and 64-bit 3073893 **2008 Server Core installation**: 32-bit 3073893 and 64-bit 3073893 **Microsoft BizTalk Server 2010**: 3073893 **Microsoft BizTalk Server 2013**: 3073893 **Microsoft BizTalk Server 2013 R2**: 3073893	15-087
Windows Shell Toolbar Object vulnerability	A vulnerability in the way Windows shell parses toolbar objects results in a remote code execution vulnerability that could be used by an attacker to gain control of a computer by tricking a user into opening a specially crafted Microsoft toolbar object. (CVE 2015-2515)	**Vista**: 3080446 **2008**: 3080446 **7**: 3080446 **2008 R2**: 3080446 **8**: 3080446 **8.1**: 3080446 **2012**: 3080446 **2012 R2**: 3080446	15-109
Unsafe Command Line Parameter Passing Vulnerability	Fixes a vulnerability which could allow information disclosure when files at a medium integrity level become accessible to Internet Explorer running in Enhanced Protection Mode (EPM). (CVE 2015-2423)	**Vista**: 3046017 and 3079757 **2008**: 3046017 and 3079757 **7**: 3046017 and 3079757 **2008 R2**: 3046017 and 3079757 **8**: 3046017 **8.1**: 3046017 **2012**: 3046017 **2012 R2**: 3046017	15-088
Microsoft Office memory corruption vulnerabilities	MS15-081 resolves vulnerabilities in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. (CVE 2015-1642 CVE 2015-2423 CVE	**Office for Mac 2011:** 3081349 **Office for Mac 2016:** 3082420	15-081

	2015-2466 CVE 2015-2467 CVE 2015-2468 CVE 2015-2469 CVE 2015-2470 CVE 2015-2477)		
Remote Code Execution in Microsoft Graphics Component	Fixes vulnerabilities in Microsoft Windows, Microsoft Office, and Microsoft Lync, the most severe of which could allow command execution when a user opens a document containing embedded OpenType fonts. (CVE 2015-2506 CVE 2015-2507 CVE 2015-2508 CVE 2015-2510 CVE 2015-2511 CVE 2015-2512 CVE 2015-2517 CVE 2015-2518 CVE 2015-2527 CVE 2015-2529 CVE 2015-2546)	**Vista**: 3087039 **Vista(gdiplus)**: 3087135 **2008**: 3087039 **2008(gdiplus)**: 3087135 **7**: 3087039 **2008 R2**: 3087039 **8**: 3087039 **8.1**: 3087039 **2012**: 3087039 **2012 R2**: 3087039 **Microsoft Lync 2013**: 3085500 **Microsoft Lync 2010**: 3081087 **Microsoft Lync 2010 Attendee**: 3081088 **Microsoft Live Meeting 2007 Console**: 3081090	15-097
Windows Task Management Elevation Of Privilege Vulnerabilities	Resolves multiple vulnerabilities that could allow elevation of privilege if a malicious attacker logs on to a target system and executes a specially crafted application. (CVE 2015-2524 CVE 2015-2525 CVE 2015-2528)	**Vista**: 3084135 3084135 (64-bit) **2008**: 3084135 3084135 (64-bit) **7**: 3084135 3084135 (64-bit) **2008 R2**: 3084135 **8**: 3082089 3084135 3082089 (64-bit) 3084135 (64-bit) **8.1**: 3082089 3084135 3082089 (64-bit) 3084135 (64-bit) **2012**: 3082089 3084135 **2012 R2**: 3082089 3084135 **10**: 3081455 3081455 (64-bit)	15-102
Multiple Windows Elevation of Privilege Vulnerabilities	MS15-111 fixes five vulnerabilities in Windows: ▪ Three elevation of privilege vulnerabilities in the way the Windows kernel handles objects in memory. An authenticated attacker who successfully exploited the vulnerabilities could run arbitrary code in kernel mode.	**Vista:** 3088195 , 3088195 (64-bit) **Server 2008:** 3088195 , 3088195 (64-bit) **7:**	15-111

	▪ An elevation of privilege vulnerability in the way Windows handles junction (or mount-point creation. An attacker who successfully exploited this vulnerability could potentially run arbitrary code in the security context of the user running a compromised application. To exploit this vulnerability, an attacker would most likely have to leverage another vulnerability that allows him to run arbitrary code in a sandboxed application. ▪ A security feature bypass vulnerability as a result of Windows failing to properly enforce the Windows Trusted Boot policy. An attacker who successfully exploited this vulnerability could disable code integrity checks, allowing test-signed executables and drivers to be loaded on a target device. (CVE 2015-2549 CVE 2015-2550 CVE 2015-2552 CVE 2015-2553 CVE 2015-2554)	3088195, 3088195 (64-bit) **Server 2008 R2:** 3088195 (64-bit) **8:** 3088195, 3088195 (64-bit) **8.1:** 3088195, 3088195 (64-bit) **Server 2012:** 3088195 (64-bit) **Server 2012 R2:** 3088195 (64-bit)	
VBScript and JScript Remote Code Execution Vulnerabilities.	MS15-108 fixes several vulnerabilities that affect JScript and VBScript scripting engines. This is achieved by addressing how they handle objects in memory and properly implementing the ASLR security feature. (CVE 2015-2482 CVE 2015-6052 CVE 2015-6055 CVE 2015-6059)	**Vista:** JScript 5.7 and VBScript 5.7 JScript 5.7 and VBScript 5.7 (64-bit) **2008:** JScript 5.8 and VBScript 5.8 JScript 5.8 and VBScript 5.8 (64-bit)	15-108
Windows Schannel TLS Triple Handshake Vulnerability	MS15-121 fixes a spoofing vulnerability that exists in all supported versions of the TLS protocol. An attacker would first have to perform a man-in-the-middle attack between the client and a legitimate server. Thereafter, the attacker could impersonate the client on any other server that uses the same credentials. (CVE 2015-6112)	**Vista:** 3081320, 3081320 (64-bit) **Server 2008:** 3081320, 3081320 (64-bit) **Windows 7:** 3081320, 3081320 (64-bit) **Server 2008 R2:** 3081320 **Windows 8:** 3081320, 3081320 (64-bit) **Windows 8.1:** 3081320, 3081320 (64-bit) **Server 2012:** 3081320 **Server 2012 R2:** 3081320	15-121
Windows NDIS Elevation of Privilege Vulnerability	MS15-117 fixes an elevation of privilege vulnerability that exists due to Network Driver Interface Standard	**Vista:** 3101722, 3101722 (64-bit) **Server 2008:**	15-117

	(NDIS) failure to check the length of a buffer prior to copying memory into it. An authenticated attacker could run a specially crafted application to gain elevated privileges on the targeted system. (CVE 2015-6098)	3101722, 3101722 (64-bit) **Windows 7:** 3101722, 3101722 (64-bit) **Server 2008 R2:** 3101722	
IPSec Denial of Service Vulnerability (MS15-120)	MS15-120 fixes a denial of service vulnerability that exists due to incorrect handling of encryption negotiation in the IPSec service. (CVE 2015-6111)	**Windows 8:** 3102939, 3102939 (64-bit) **Windows 8.1:** 3102939, 3102939 (64-bit) **Windows 2012:** 3102939 **Windows 2012 R2:** 3102939	15-120
Windows Security Feature Bypass Vulnerability (MS15-115)	MS15-115 fixes a vulnerability in Microsoft Windows which could allow an attacker to bypass security features if the attacker convinces a user to open a specially crafted document or to visit an untrusted webpage that contains embedded fonts. (CVE 2015-6113)	**Windows Vista:** 3101746 3101746 (64-bit) **Windows 2008:** 3101746 3101746 (64-bit) **Windows 7:** 3101746 3101746 (64-bit) **Windows 2008 R2:** 3101746 **Windows 8:** 3101746 3101746 (64-bit) **Windows 2012:** 3101746 **Windows 8.1:** 3101746 3101746 (64-bit) **Windows 2012 R2:** 3101746 **Windows 10:** 3105213 3105213 (64-bit)	15-115
Windows Susceptibility to Malicious Content (MS15-115)	MS15-115 fixes several vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to open a specially crafted document or to visit an untrusted webpage that contains embedded fonts. (CVE 2015-6100 CVE 2015-6101 CVE 2015-6102 CVE 2015-6103 CVE 2015-6104 CVE 2015-6109)	**Windows Vista:** 3097877 3097877 (64-bit) **Windows 2008:** 3097877 3097877 (64-bit) **Windows 7:** 3097877 3097877 (64-bit) **Windows 2008 R2:** 3097877 **Windows 8:** 3097877 3097877 (64-bit)	15-115

		Windows 2012: 3097877 **Windows 8.1:** 3097877 3097877 (64-bit) **Windows 2012 R2:** 3097877 **Windows 10:** 3105213 3105213 (64-bit)	
Winsock Elevation of Privilege Vulnerability	MS15-119 fixes an elevation of privilege vulnerability which could allow Winsock to make a call to a memory address without verifying that the address is valid. (CVE 2015-2478)	**Windows Vista:** KB3092601, KB3092601 (64-bit) **Windows Server 2008:** KB3092601, KB3092601 (64-bit) **Windows 7:** KB3092601, KB3092601 (64-bit) **Windows Server 2008 R2:** KB3092601 (64-bit) **Windows 8:** KB3092601, KB3092601 (64-bit) **Windows 8.1:** KB3092601, KB3092601 (64-bit) **Windows Server 2012:** KB3092601 (64-bit) **Windows Server 2012 R2:** KB3092601 (64-bit) **Windows 10:** KB3105213, KB3105211	15-119
Microsoft SharePoint vulnerabilities	Fixes three memory corruption vulnerabilities in SharePoint Excel Services and Word Automation Services which could allow arbitrary code to run in the context of the current user. (CVE 2015-6038 CVE 2015-6093 CVE 2015-6094)	**2007:** 3101559 **2010:** 3101525 **2010:** 3085511 **2013:** 3101364 **2013:** 3085477	15-116
Multiple Microsoft Office Memory Corruption vulnerabilities	Fixes six memory corruption vulnerabilities in Microsoft Office which could allow arbitrary code to run in the context of the current user. (CVE 2016-0022 CVE 2016-0052 CVE 2016-0053 CVE 2016-0054 CVE	Microsoft Security Bulletin 16-015 2007 Office Suite: https://support.microsoft.com/en-us/kb	16-015

2016-0055 CVE 2016-0056)

/3114742 Office 2010: https://support.microsoft.com/en-us/kb/3114752 Word 2007: Word 2010: https://www.microsoft.com/en-us/download/details.aspx?id=50873 Excel 2013 (KB3114734) 32-Bit Edition; https://www.microsoft.com/en-us/download/details.aspx?id=50941 Excel 2013 (KB3114734) 64-Bit Edition Word 2013: https://www.microsoft.com/en-us/download/details.aspx?id=50902 Word 2013 (KB3114724) 32-Bit Edition; https://www.microsoft.com/en-us/download/details.aspx?id=51012 Word 2013 (KB3114724) 64-Bit Edition Word 2016: https://www.microsoft.com/en-us/download/details.aspx?id=50945 Word 2016 (KB3114702) 32-Bit Edition; https://www.microsoft.com/en-us/download/details.aspx?id=50891 Word 2016 (KB3114702) 64-Bit Edition Excel 2007: https://www.microsoft.com/en-us/download/details.aspx?id=51015 Excel 2007 (KB3114741) Excel 2010: https://www.microsoft.com/en-us/download/details.aspx?id=5

		1011 (KB3114759) 32-Bit Edition, https://www.microsoft.com/en-us/download/details.aspx?id=50914 (KB3114759) 64-Bit Edition Excel 2013: https://www.microsoft.com/en-us/download/details.aspx?id=50873 Excel 2013 (KB3114734) 32-Bit Edition; https://www.microsoft.com/en-us/download/details.aspx?id=50941 Excel 2013 (KB3114734) 64-Bit Edition Excel 2016: https://www.microsoft.com/en-us/download/details.aspx?id=51002 Excel 2016 (KB3114698) 32-Bit Edition; https://www.microsoft.com/en-us/download/details.aspx?id=50870 Excel 2016 (KB3114698) 64-Bit Edition	
Multiple Library Loading vulnerabilities	Fixes three vulnerabilities which could allow an attacker with local system access to take complete control of the target. (CVE 2015-6128 CVE 2015-6132 CVE 2015-6133)	**Vista**: 3108371 and 3108381 **2008**: 3108371 and 3108381 **7**: 3108371 and 3108381 **2008 R2**: 3108371 and 3108381 **8**: 3108347 and 3108381 **8.1**: 3108347 and 3108381 **2012**: 3108347 and 3108381 **2012 R2**: 3108347 and 3108381 **10**: 3116869 **10 v1511**: 3116900	15-132
Secondary Logon Elevation of Privilege (MS16-032)	This update resolves an issue with the way Windows manages request handles in memory. An attacker could	**Vista** 3139914 3139914 (64-bit) **2008** 3139914	16-032

	abuse the design flaw to elevate privileges by causing Windows Secondary Logon Service to fail. (CVE 2016-0099)	3139914 (64-bit) **7** 3139914 3139914 (64-bit) **2008 R2** 3139914 **8.1** 3139914 3139914 (64-bit) **2012** 3139914 **2012 R2** 3139914 **10**: 3140745	
`ActiveSyncProvider` Information Disclosure Vulnerability (MS16-103)	This update resolves an information disclosure vulnerability in Microsoft Windows. Exploitation of the vulnerability would cause information disclosure when Universal Outlook fails to establish a secure connection. (CVE 2016-3312)	**Windows 10** 3176492 **Windows 10 (v1511)** 3176493	16-103
Secondary Logon Elevation of Privilege (MS16-046)	This update resolves a vulnerability in Microsoft Windows by correcting how Windows Secondary Logon Service handles requests in memory. An attacker who successfully exploits this vulnerability could potentially run malicious code. (CVE 2016-0135)	**Windows 10** 3147461 **Windows 10 (v1511)** 3147458	16-046
Microsoft Windows Insecure Library Loading Vulnerability (MS16-025)	This update resolves a vulnerability in Microsoft Windows which could allow remote code execution if Windows fails to properly validate input before loading certain libraries. However, an attacker must first gain access to the local system with the ability to execute a malicious application. (CVE 2016-0100)	**Vista** 3140709, 3140709 (64-bit) **2008** 3140709, 3140709 (64-bit)	16-025
Windows Graphic Fonts vulnerability (MS16-026)	This update resolves a remote code execution vulnerability when an attacker is able to convince a user to open a crafted document or webpage. The vulnerability exists in embedded OpenType fonts. (CVE 2016-0120 CVE 2016-0121)	**Vista** 3140735 3140735 (64-bit) **2008** 3140735 3140735 (64-bit) **7** 3140735 3140735 (64-bit) **2008 R2** 3140735 **8.1** 3140735 3140735 (64-bit) **2012** 3140735 **2012 R2** 3140735 **10**: 3140745	16-026
Graphics Memory Corruption Vulnerabilities	Multiple vulnerabilities in the Microsoft Graphics Component could allow command execution when a user opens a specially crafted document or web page. (CVE 2015-6106 CVE 2015-6107 CVE 2015-6108)	15-128	15-128
VBScript and JScript Remote Code Execution Vulnerability (MS15-126)	MS15-126 fixes two vulnerabilities in the VBScript and JScript engines, the most severe of which could lead to remote code execution due to improper handling of specially crafted website content. (CVE 2015-6135 CVE 2015-6136)	**Vista**: 3105579 3105579 (64-bit) **Windows 2008**: 3105579 3105579 (64-bit) **Windows 2008 R2**: 3105578 (64-bit)	15-126

Multiple Windows Kernel Mount Point Elevation of Privilege Vulnerabilities	MS16-008 fixes two vulnerabilities in the Windows kernel which can be triggered while validating reparse points being set by sandbox applications. The vulnerabilities could allow elevation of privilege if an attacker logs on to a vulnerable system and runs a specially crafted application. (CVE 2016-0006 CVE 2016-0007)	**Vista**: 3121212, 3121212 (64-bit) **Server 2008**: 3121212, 3121212 (64-bit) **Windows 7**: 3121212, 3121212 (64-bit) **Server 2008 R2**: 3121212 (64-bit) **Windows 8**: 3121212, 3121212 (64-bit) **Windows 8.1**: 3121212, 3121212 (64-bit) **Server 2012**: 3121212 (64-bit) **Server 2012 R2**: 3121212 (64-bit)	16-008
Windows Kernel Elevation of Privilege Vulnerability (MS16-060)	MS16-060 fixes a vulnerability in the Windows kernel which could allow elevation of privilege if an attacker is able to log on to a target system and run a specially crafted application. (CVE 2016-0180)	**Vista**: 3153171, 3153171 (64-bit) **Server 2008**: 3153171, 3153171 (64-bit) **Windows 7**: 3153171, 3153171 (64-bit) **Server 2008 R2**: 3153171 (64-bit) **Windows 8.1**: 3153171, 3153171 (64-bit) **Server 2012**: 3153171 (64-bit) **Server 2012 R2**: 3153171 (64-bit) **Windows 10**: 3156387 3156387 (64-bit)	16-060
Windows Remote Procedure Call Elevation of Privilege Vulnerability (MS16-061)	MS16-061 fixes a vulnerability in Windows RPC which could allow elevation of privilege. Exploitation does not require authentication. (CVE 2016-0178)	**Vista**: 3153171, 3153171 (64-bit) **Server 2008**: 3153171, 3153171 (64-bit) **Windows 7**: 3153171, 3153171 (64-bit) **Server 2008 R2**: 3153171 (64-bit) **Windows 8.1**: 3153704, 3153704 (64-bit) **Server 2012**: 3153704 (64-bit) **Server 2012 R2**: 3153704 (64-bit)	16-061

		Windows 10: 3156387 3156387 (64-bit)	
Windows Kernel Elevation of Privilege Vulnerability (MS16-031)	MS16-031 fixes a vulnerability in the Windows kernel which could allow elevation of privilege if an attacker is able to log on to a target system and run a specially crafted application. (CVE 2016-0087)	**Vista**: 3140410, 3140410 (64-bit) **Server 2008**: 3140410, 3140410 (64-bit) **Windows 7**: 3140410, 3140410 (64-bit) **Server 2008 R2**: 3140410 (64-bit)	16-031
Multiple Remote Code Execution vulnerabilities	Fixes multiple remote code execution vulnerabilities which could allow an attacker to take complete control of the target. (CVE 2016-0014 CVE 2016-0015 CVE 2016-0016 CVE 2016-0018 CVE 2016-0019 CVE 2016-0020)	**Vista**: 3121918, 3109560, 3110329, 3108664 or 3121918 (64-bit), 3109560 (64-bit), 3110329 (64-bit), 3108664 (64-bit). **Server 2008**: 3121918, 3109560, 3110329, 3108664 or 3121918 (64-bit), 3109560 (64-bit), 3110329 (64-bit), 3108664 (64-bit). **Windows 7**: 3121918, 3109560, 3110329, 3121461, 3108664 or 3121918 (64-bit), 3109560 (64-bit), 3110329 (64-bit), 3121461 (64-bit), 3108664 (64-bit). **Server 2008 R2**: 3121918 (64-bit), 3109560 (64-bit), 3110329 (64-bit), 3108664 (64-bit). **Windows 8**: 3121918, 3109560, 3110329, 3121461 or 3121918 (64-bit), 3109560 (64-bit), 3110329 (64-bit), 3121461 (64-bit). **Windows 8.1**: 3121918, 3109560,	16-007

		3110329, 3121461 or 3121918 (64-bit), 3109560 (64-bit), 3110329 (64-bit), 3121461 (64-bit). **Server 2012**: 3121918, 3109560, 3110329. **Server 2012 R2**: 3121918 (64-bit), 3109560 (64-bit), 3110329 (64-bit), 3121461 (64-bit).	
VBScript and JScript Remote Code Execution Vulnerability (MS16-003)	MS16-003 fixes vulnerabilities in the VBScript scripting engine, the most severe of which could lead to remote code execution due to improper handling of specially crafted website content. (CVE 2016-0002)	**Vista**: 3124624 3124624 (64-bit) **Windows 2008**: 3124624 3124624 (64-bit) **Windows 2008 R2**: 3124624 (64-bit)	16-003
Windows GDI32.dll ASLR Bypass Vulnerability (MS16-005)	MS16-005 fixes an ASLR bypass vulnerability which exists because Windows graphic device interface fails to handle specially crafted websites correctly. (CVE 2016-0008)	**Vista**: 3124001 3124001 (64-bit) **Windows 2008**: 3124001 3124001 (64-bit) **Windows 2008 R2**: 3124001 **Windows 7**: 3124001 3124001 (64-bit) **Windows 8**: 3124001 3124001 (64-bit) **Windows 8.1**: 3124001 3124001 (64-bit) **Windows 2012**: 3124001 **Windows 2012 R2**: 3124001	16-005
Visual Basic Security Feature Bypass Vulnerability (MS16-004)	MS16-004 fixes a security feature bypass vulnerability which exists because Microsoft Office fails to use the ASLR security feature in certain cases. (CVE 2016-0012)	**VB**: 3096896	16-004
Win32k Remote Code Execution Vulnerability (MS16-005)	MS16-005 fixes a remote code execution vulnerability that exists due to Windows improperly handling specially crafted websites. (CVE 2016-0009)	**Vista**: 3124000 3124000 (64-bit) **Windows 2008**: 3124000 3124000 (64-bit) **Windows 2008 R2**: 3124000 **Windows 7**: 3124000 3124000 (64-bit)	16-005

		Windows 10: 3124000 3124000 (64-bit)	
Microsoft Windows PDF Library Remote Code Execution Vulnerability (MS16-012)	MS16-012 fixes vulnerabilities in Microsoft Windows which could allow remote code execution if Windows PDF Library improperly handles application programming interface calls, which could then allow arbitrary code to run in the context of the current user. (CVE 2016-0058 CVE 2016-0046)	**Windows8.1**: 3123294 3123294 (64-bit) **Windows Server 2012**: 3123294 **Windows 2012 R2**: 3123294 **Windows 10**: 3135174 3135174 (64-bit)	16-012
Windows Media Center Remote Code Execution Vulnerability (MS15-134)	MS15-134 fixes two vulnerabilities in Windows Media Center, the most severe of which could lead to remote code execution due to improper handling of specially crafted media center link files. (CVE 2015-6127 CVE 2015-6131)	**Vista**: 3108669 3108669 (64-bit) **Windows 7**: 3108669 3108669 (64-bit) **Windows 8**: 3108669 3108669 (64-bit) **Windows 8.1**: 3108669 3108669 (64-bit)	15-134
Windows Journal Memory Corruption Vulnerability (MS16-013)	Addresses a vulnerability which could allow remote code execution if a user opens a specially crafted Journal file. (CVE 2016-0038)	**Vista**: KB3115858 KB3115858 (64-bit) **2008**: KB3115858 KB3115858 (64-bit) **7**: KB3115858 KB3115858 (64-bit) **2008 R2**: KB3115858 **Windows 8.1**: KB3115858 KB3115858 (64-bit) **Windows 2012**: KB3115858 **Windows 2012 R2**: KB3115858	16-013
WebDAV Elevation of Privilege Vulnerability (MS16-016)	MS16-016 fixes a vulnerability in Microsoft Web Distributed Authoring and Versioning (WebDAV) client when WebDAV improperly validates input. An attacker who successfully exploited this vulnerability could execute arbitrary code with elevated permissions. (CVE 2016-0051)	**Vista**: KB3124280 KB3124280 (64 bit) **2008**: KB3124280 KB3124280 (64 bit) **7**: KB3124280 KB3124280 (64 bit) **2008 R2**: KB3124280 **Windows 8.1**: KB3124280 KB3124280 (64 bit)	16-016

		Windows 2012: KB3124280 **Windows 2012 R2**: KB3124280 **Windows 10:** 3135174 3135174 (64-bit)	
Windows RDP Display Driver Privilege Elevation Vulnerability (MS16-017)	MS16-017 fixes a vulnerability in Windows Remote Desktop Display Driver which could allow elevation of privilege if an authenticated attacker logs on to the target system using RDP and sends specially crafted data over the connection. (CVE 2016-0036)	**Windows 7**: KB3126446 KB3126446 (64 bit) **Windows 8.1**: KB3126446 KB3126446 (64 bit) **Windows 2012**: KB3126446 **Windows 2012 R2**: KB3126446 **Windows 10:** 3135174 3135174 (64-bit)	16-017
Windows DLL Loading Remote Code Execution Vulnerability (MS16-014)	MS16-014 fixes a remote code execution vulnerability that exists due to Windows improperly handling input before loading DLL files. (CVE 2016-0041)	**Vista**: 3126587 3126587 (64-bit) **2008**: 3126587 3126587 (64-bit) **7**: 3126587 3126587 (64-bit) **2008 R2**: 3126587 **Windows 8.1**: 3126587 3126587 (64-bit) **Windows 2012**: 3126587 **Windows 2012 R2**: 3126587 **Windows 10:** 3135174	16-014
Kerberos DLL Loading Remote Code Execution Vulnerability (MS16-014)	MS16-014 fixes two vulnerabilities the most severe of which could allow remote code execution. This vulnerability exists due to Windows improperly handling input before loading DLL files. (CVE 2016-0042 CVE 2016-0049)	**Vista**: 3126041 3126041 **2008**: 3126041 3126041 **Windows 8.1**: 3126041 3126041 **Windows 2012 R2**: 3126041	16-014
Multiple vulnerabilities in Ntoskrnl executable (MS16-014)	MS16-014 fixes multiple vulnerabilities the most severe of which could allow remote code execution. This vulnerability exists due to Windows improperly handling input before loading DLL files. (CVE 2016-0040 CVE 2016-0042 CVE 2016-0049)	**Vista**: 3126593 3126593 (64-bit) **2008**: 3126593 3126593 (64-bit) **7**: 3126593 3126593 (64-bit) **2008 R2**: 3126593 **Windows 8.1**: 3126593 3126593 (64-bit) **Windows 2012**: 3126593	16-014

		Windows 2012 R2: 3126593 **Windows 10:** 3135174	
Windows DLL Loading Denial of Service Vulnerability (MS16-014)	MS16-014 fixes a denial of service vulnerability that exists due to the way Microsoft Sync Framework handles specially crafted files. (CVE 2016-0044)	**Windows 8.1**: 3126434 3126434 (64-bit) **Windows 2012 R2**: 3126434	16-014
Win32k Elevation Of Privilege Vulnerability (MS16-018)	MS16-018 fixes a vulnerability in the Windows kernel-mode driver that could otherwise allow an attacker to run malicious code in kernel mode. (CVE 2016-0048)	**Vista**: KB3134214 KB3134214 (64 bit) **2008**: KB3134214 KB3134214 (64 bit) **7**: KB3134214 KB3134214 (64 bit) **2008 R2**: KB3134214 **Windows 8.1**: KB3134214 KB3134214 (64 bit) **Windows 2012**: KB3134214 **Windows 2012 R2**: KB3134214 **Windows 10:** 3135174 3135174 (64-bit)	16-018
Active Directory Federation Services Denial Of Service Vulnerability (MS16-020)	MS16-020 fixes a vulnerability in Active Directory Federation Services (ADFS) that could potentially allow denial of service only if the attacker succeeds in sending certain input data during forms-based authentication to an ADFS server. (CVE 2016-0037)	**Windows 2012 R2**: KB3134222	16-020
Windows Media parsing vulnerabilities	Fixes two vulnerabilities which could allow remote code execution if a user opens a specially crafted media file. (CVE 2016-0098 CVE 2016-0101)	**7**: 3138910, 3138962 **2008 R2**: 3138910, 3138962 **8.1**: 3138910, 3138962 **2012**: 3138910, 3138962 **2012 R2**: 3138910, 3138962	16-027
Microsoft Windows PDF Library Remote Code Execution Vulnerability (MS16-028)	Fixes vulnerabilities which if left unattended could allow remote code execution if a user opens a specially crafted .pdf file. If the attacker is successful in their exploitation attempt, it would allow arbitrary code execution in the context of the current user. (CVE 2016-0117 CVE 2016-0118)	**Windows 8.1**: KB3137513, KB3137513 (64-bit) **Windows 2012**: KB3137513 **Windows 2012 R2**: KB3138910 **Windows 10**: KB3130745,	16-028

		KB3130745 (64-bit)	
Microsoft Windows PDF Library Remote Code Execution Vulnerability (MS16-102)	MS16-102 resolves a remote code execution vulnerability in the Windows PDF Library. An attacker that entices a user to open a specially crafted PDF file could execute arbitrary code in the context of the current user. (CVE 2016-3319)	**Windows 8.1**: KB3175887, KB3137513 (64-bit) **Windows 2012**: KB3175887 **Windows 2012 R2**: KB3175887 **Windows 10**: KB3176492	16-102
Windows OLE Memory Remote Code Execution (MS16-030)	Fixes vulnerabilities which could allow remote code execution if Windows OLE fails to properly validate user input. (CVE 2016-0091 CVE 2016-0092)	**Vista:** 3139940 3139940 (64-bit) **2008:** 3139940 3139940 (64-bit) **7:** 3139940 3139940 (64-bit) **2008 R2:** 3139940 (64-bit) **8.1:** 3139940 3139940 (64-bit) **2012:** 3139940 **2012 R2:** 3139940 **Windows 10** KB3140745 KB3140768	16-030
Word Automation Services vulnerability	Fixes a command execution vulnerability in SharePoint Server and Office Web Apps 2010 and 2013. (CVE 2016-0134)	**SharePoint Server 2010:** 3114866 **SharePoint Server 2013:** 3114814 **Office Web Apps 2010:** 3114880 **Office Web Apps 2013:** 3114821	16-029
USB Mass Storage Elevation of Privilege Vulnerability	This security update resolves an elevation of privilege vulnerability that is due to the failure of the Windows USB Mass Storage Class driver to properly validate objects in memory. A local attacker with physical access to the vulnerable system could insert a specially crafted USB device. If the exploit is successful, the attacker could run arbitrary code in kernel mode. (CVE 2016-0133)	**Vista**: KB3139398 KB3139398 (64 bit) **2008**: KB3139398 KB3139398 (64 bit) **7**: KB3139398 KB3139398 (64 bit) **2008 R2**: KB3139398 **Windows 8.1**: KB3139398 KB3139398 (64 bit) **Windows 2012**: KB3139398 **Windows 2012 R2**: KB3139398 **Windows 10**:	16-033

		KB3139398	
Win32k Elevation Of Privilege Vulnerability (MS16-034)	Resolves vulnerabilities in the Windows kernel-mode driver by correcting how Windows handles objects in memory that could otherwise allow an attacker to run malicious code. (CVE 2016-0093 CVE 2016-0094 CVE 2016-0095 CVE 2016-0096)	**Vista**: KB3139852 KB3139852 (64 bit) **2008**: KB3139852 KB3139852 (64 bit) **7**: KB3139852 KB3139852 (64 bit) **2008 R2**: KB3139852 **Windows 8.1**: KB3139852 KB3139852 (64 bit) **Windows 2012**: KB3139852 **Windows 2012 R2**: KB3139852 **Windows 10:** KB3140745 KB3140745 (64-bit)	16-034
Win32k Elevation Of Privilege Vulnerability (MS16-039)	Resolves vulnerabilities in Microsoft Windows by correcting how Windows font library handles embedded fonts with the most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted malicious document. (CVE 2016-0143 CVE 2016-0145 CVE 2016-0165 CVE 2016-0167)	**Vista**: KB3145739 KB3145739 (64 bit) **2008**: KB3145739 KB3145739 (64 bit) **Windows 7**: KB3145739 KB3145739 (64 bit) **2008 R2**: KB3145739 **Windows 8.1**: KB3145739 KB3145739 (64 bit) **Windows 2012**: KB3145739 **Windows 2012 R2**: KB3145739 **Windows 10:** KB3147461 KB3147458	16-039
Microsoft XML Core Services Remote Code Execution Vulnerability (MS16-040)	Addresses a vulnerability that could otherwise allow remote code execution using a specially craft link. The update resolves this by correcting how the MSXML parser handles user input. (CVE 2016-0147)	**Vista**: KB3146963 KB3146963 (64 bit) **2008**: KB3146963 KB3146963 (64 bit) **7**: KB3146963 KB3146963 (64 bit) **2008 R2**: KB3146963	16-040

		Windows 8.1: KB3146963 KB3146963 (64 bit) **Windows 2012**: KB3146963 **Windows 2012 R2**: KB3146963 **Windows 10:** KB3147461	
Windows SAM and LSAD Downgrade Vulnerability (MS16-047)	Resolves a vulnerability that allows elevation of privilege from a man-in-the-middle attack. The patch resolves how the SAM and LSAD handle authentication levels. (CVE 2016-0128)	**Vista**: KB3149090 KB3149090 (64 bit) **2008**: KB3149090 KB3149090 (64 bit) **7**: KB3149090 KB3149090 (64 bit) **2008 R2**: KB3149090 **Windows 8.1**: KB3149090 KB3149090 (64 bit) **Windows 2012**: KB3149090 **Windows 2012 R2**: KB3149090 **Windows 10:** KB3147461	16-047
Windows HTTP.sys Denial of Service Vulnerability	Fixes a vulnerability in Windows which could allow denial of service if an attacker sends a specially crafted HTTP packet to a target system. (CVE 2016-0150)	**Windows 10**: 3148795	16-049
Windows CSRSS Security Feature Bypass	Fixes a vulnerability in Windows which could allow a logged-on user to run arbitrary code as administrator. (CVE 2016-0151)	**8.1**: 3146723 **2012**: 3146723 **2012 R2**: 3146723 **10**: 3147461 **10 Version 1511**: 3147458	16-048
Windows OLE Remote Code Execution Vulnerability	Fixes a vulnerability in Windows which could allow remote code execution if Windows OLE fails to properly validate user input. (CVE 2016-0153)	**Vista**: 3146706 3146706 (64 bit) **2008**: 3146706 3146706 (64 bit) **7**: 3146706 3146706 (64 bit) **2008 R2**: 3146706 **Windows 8.1**: 3146706 3146706 (64 bit) **Windows 2012**: 3146706 **Windows 2012 R2**: 3146706 (64 bit)	16-044

VBScript and JScript Remote Code Execution Vulnerability (MS16-069)	MS16-069 resolves vulnerabilities in the JScript and VBScript scripting engines that could otherwise allow an attacker control of an affected system and could allow remote code execution if a user visits a malicious website. (CVE 2016-3205 CVE 2016-3206 CVE 2016-3207)	**Vista**: 3158364, 3158364 (64-bit) **Windows Server 2008**: 3158364, 3158362 (64-bit)	16-069
VBScript and JScript Remote Code Execution Vulnerability (MS16-053)	MS16-053 resolves vulnerabilities in the JScript and VBScript scripting engines that could otherwise allow an attacker control of an affected system. (CVE 2016-0187 CVE 2016-0189)	**Vista**: 3158991, 3158991 (64-bit) **Windows 2008**: 3158991, 3158991 (64-bit)	16-053
Microsoft Windows Media Center Remote Code Execution Vulnerability (MS16-059)	Fixes a vulnerability which could allow remote code execution when a specially crafted Windows Media Center file is opened. (CVE 2016-0185)	**Vista**: 3150220 3150220 (64-bit) **Windows 7**: 3150220 3150220 (64-bit) **Windows 8.1**: 3150220 3150220 (64-bit)	16-059
Microsoft Windows Journal Remote Code Execution Vulnerability (MS16-056)	Fixes a vulnerability which could allow remote code execution when a specially crafted Journal file is opened. (CVE 2016-0182)	**Vista**: 3155178 3155178 (64-bit) **Windows 7**: 3155178 3155178 (64-bit) **Windows 8.1**: 3155178 3155178 (64-bit) **Windows 10**: 3156387	16-056
Graphics Memory Corruption Vulnerability	Fixes a vulnerability which could allow remote code execution when the Windows font library improperly handles specially crafted embedded fonts. (CVE 2016-0145)	**Skype for Business 2016**: 3114960 3114960 (64 bit) **Lync 2013**: 3114944 3114944 (64 bit) **Lync 2010**: 3144427 3144427 (64 bit) **Live Meeting 2007 Console**: KB 3144432	16-039
Windows Graphics Component Vulnerabilities (MS16-055)	MS16-055 fixes two information disclosure vulnerabilities and one remote code execution vulnerability. The security update addresses these vulnerabilities by correcting how the Windows GDI component handle objects in memory. (CVE 2016-0168 CVE 2016-0169 CVE 2016-0170)	**Vista**: 3156013 3156013 (64-bit) **Windows 2008**: 3156013 3156013 (64-bit) **Windows 2008 R2**: 3156013 **Windows 7**: 3156013 3156013 (64-bit) **Windows 8.1**: 3156013 3156013 (64-bit) **Windows 2012**:	16-055

		3156013 **Windows 2012 R2**: 3156013	
Direct3D Use After Free Vulnerability (MS16-055)	Fixes a vulnerability which could allow code execution when a user visits a specially crafted website. (CVE 2016-0184)	**Vista**: 3156016 3156016 (64-bit) **Windows 2008**: 3156016 3156016 (64-bit) **Windows 2008 R2**: 3156016 **Windows 7**: 3156016 3156016 (64-bit) **Windows 8.1**: 3156016 3156016 (64-bit) **Windows 2012**: 3156016 **Windows 2012 R2**: 3156016	16-055
Windows Imaging Component Memory Corruption Vulnerability (MS16-055)	Fixes a vulnerability which could allow code execution when a user visits a specially crafted website. (CVE 2016-0195)	**Vista**: 3156019 3156019 (64-bit) **Windows 2008**: 3156019 3156019 (64-bit) **Windows 2008 R2**: 3156019 **Windows 7**: 3156019 3156019 (64-bit) **Windows 8.1**: 3156019 3156019 (64-bit) **Windows 2012**: 3156019 **Windows 2012 R2**: 3156019	16-055
Windows Shell remote code execution	Fixes a vulnerability which could allow code execution when a user visits a specially crafted website. (CVE 2016-0179)	**8.1**: 3156059 **2012 R2**: 3156059 **10**: 3156387 **10 Version 1511**: 3156421	16-057
Windows DLL Loading Remote Code Execution Vulnerability (MS16-058)	Resolves a vulnerability which could allow remote code execution if an attacker with access to the local system executes a malicious application. (CVE 2016-0152)	**Vista**: 3141083 3141083 (64-bit) **Windows 2008**: 3141083 3141083 (64-bit)	16-058
Windows Kernel-Mode Driver Vulnerabilities fixed by MS16-062	Resolves various vulnerabilities in Microsoft Windows that could allow elevation of privilege or information disclosure if a logged-on user runs a specially crafted application on the affected target. (CVE 2016-0171 CVE 2016-0173 CVE 2016-0174 CVE 2016-0175 CVE 2016-0176 CVE 2016-0196 CVE 2016-0197)	**Vista**: KB3153199, KB3156017 KB3153199 (64 bit), KB3156017 (64 bit) **2008**: KB3153199, KB3156017 KB3153199 (64 bit), KB3156017 (64 bit) **7**: KB3153199,	16-062 (superseded by 16-073)

		KB3156017 KB3153199 (64 bit), KB3156017 (64 bit) **2008 R2**: KB3153199 (64 bit), KB3156017 (64 bit) **Windows 8.1**: KB3153199, KB3156017 KB3153199 (64 bit), KB3156017 (64 bit) **Windows 2012**: KB3153199 (64 bit), KB3156017 (64 bit) **Windows 2012 R2**: KB3153199 (64 bit), KB3156017 (64 bit) **Windows 10:** KB3156387, KB3156387 (64-bit)	
Windows Kernel-Mode Driver Vulnerabilities fixed by MS16-073	Resolves two privilege elevation vulnerabilities in the Windows kernel Win32k driver and one information disclosure vulnerability in Windows Virtual PCI. In order to exploit these vulnerabilities, an attacker would have to log on to the vulnerable system and run a specially crafted application. (CVE 2016-3218 CVE 2016-3221 CVE 2016-3232)	**Vista**: KB3161664, KB3161664 (64 bit) **2008**: KB3161664, KB3161664 (64 bit) **7**: KB3161664, KB3161664 (64 bit) **2008 R2**: KB3161664 (64 bit) **Windows 8.1**: KB3161664, KB3161664 (64 bit) **Windows 2012**: KB3161664 (64-bit), KB3164294 (64 bit) **Windows 2012 R2**: KB3161664 (64-bit), KB3164294 (64 bit) **Windows 10:** KB3161664	16-073 (superseded by 16-090)
Windows Kernel-Mode Driver Vulnerabilities fixed by MS16-090	Resolves five privilege elevation vulnerabilities in the Windows kernel Win32k driver and one Information	**Vista**: KB3168965, KB3168965 (64 bit)	16-090

	Disclosure Vulnerability. For these vulnerabilities to be exploited, an attacker would have to log on to the vulnerable system and run a specially crafter application. (CVE 2016-3249 CVE 2016-3250 CVE 2016-3251 CVE 2016-3252 CVE 2016-3254 CVE 2016-3286)	**2008**: KB3168965, KB3168965 (64 bit) **7**: KB3168965, KB3168965 (64 bit) **2008 R2**: KB3168965 **Windows 8.1**: KB3168965, KB3168965 (64 bit) **Windows 2012**: KB3168965 **Windows 2012 R2**: KB3168965 **Windows 10:** KB3163912, KB3172985 (v1511)	
Windows WPAD Elevation of Privilege Vulnerabilities (MS16-077)	Resolves three privilege elevation vulnerabilities in the way Windows handles proxy discovery and Web Proxy Auto Discovery (WPAD) automatic proxy detection. (CVE 2016-3213 CVE 2016-3236 CVE 2016-3299)	**Vista**: KB3161949, KB3161949 (64 bit) **2008**: KB3161949, KB3161949 (64 bit) **7**: KB3161949, KB3161949 (64 bit) **2008 R2**: KB3161949 (64 bit) **Windows 8.1**: KB3161949, KB3161949 (64 bit) **Windows 2012**: KB3161949 (64-bit) **Windows 2012 R2**: KB3161949 (64-bit) **Windows 10:** KB3161949	16-077
Hypervisor Code Integrity Security Feature Bypass	Windows incorrectly allows certain kernel-mode pages to be marked as Read, Write, Execute (RWX) even with Hypervisor Code Integrity (HVCI) enabled, allowing an attacker to run a specially crafted application which bypasses code integrity protections in Windows. (CVE 2016-0181)	**10**: 3156387 **10 Version 1511**: 3156421	16-066
Windows Kernel Information Disclosure Vulnerability (MS16-089)	Microsoft Windows Secure Kernel fails to handle certain objects in memory correctly which can lead to information disclosure. (CVE 2016-3256)	**Windows 10**: 3163912 **Windows 10 Version 1511**: 3172985	16-089

Windows Diagnostics Hub Elevation of Privilege Vulnerability (MS16-078)	Microsoft Diagnostics Hub on Windows 10 fails to properly sanitize input which an attacker could exploit to gain elevated privileges. (CVE 2016-3231)	**Windows 10**: 3163017 **Windows 10 Version 1511**: 3163018	16-078
Remote Desktop Protocol Drive Redirection information disclosure	Windows does not correctly tie a USB disk mounted over Remote Desktop Protocol (RDP) via Microsoft RemoteFX to the session of the mounting user, allowing an attacker to obtain access to file and directory information on the mounting user's USB disk. (CVE 2016-0190)	**8.1**: 3155784 **2012**: 3155784 **2012 R2**: 3155784	16-067
Windows Kernel Local Elevation Privilege Vulnerabilities	Resolves multiple vulnerabilities which could allow a user access to sensitive registry information. (CVE 2016-0070 CVE 2016-0073 CVE 2016-0075 CVE 2016-0079	**Vista**: KB3191256, KB3191256 (64-bit) **Windows 2008** KB3191256, KB3191256 (64-bit) **Windows 2008 R2**: KB3192391 **Windows 7**: KB3192391, KB3185330, KB3192391 (64-bit), KB3185330 (64-bit) **Windows 8.1**: KB3192392, KB3185331, KB3192392 (64-bit), KB3185331 (64-bit) **Windows 2012**: KB3192393, KB3195332 **Windows 2012 R2**: KB3192392, KB3182392 (64-bit) **Windows 10**: KB3192440, KB3192440_(64-bit)	16-124
Windows SMB Server Elevation of Privilege Vulnerability (MS16-075)	This patch addresses the vulnerability by fixing how Windows Server Message Block Server handles credential forwarding requests which could otherwise allow an elevation of privilege attack. (CVE 2016-3225)	**Vista**: 3161561, 3161561 (64-bit) **Windows 2008** 3161561, 3161561 (64-bit) **Windows 2008 R2**: 3161561 **Windows 7**: 3161561, 3161561 (64-bit) **Windows 8.1**:	16-075

		3161561, 3161561 (64-bit) **Windows 2012**: 3161561 **Windows 2012 R2**: 3161561	
Windows Netlogon Memory Corruption Remote Code Execution Vulnerability (MS16-076)	This update addresses the vulnerability by resolving how Netlogon handles the establishment of secure channels which could otherwise allow an remote code execution attack. (CVE 2016-3228)	**Windows 2008**: 3161561, 3161561 (64-bit) **Windows 2008 R2**: 3161561 **Windows 8.1**: 3161561, 3161561 (64-bit) **Windows 2012**: 3161561 **Windows 2012 R2**: 3162343	16-076
Group Policy Elevation of Privilege Vulnerability	Fixes a vulnerability when Microsoft Windows processes group policy updates. The vulnerability could allow a man-in-the-middle attack against the traffic passing between a domain controller and the target machine. (CVE 2016-3223)	**Vista:** KB3159398, KB3159398 (64 bit), **2008:** KB3159398, KB3159398 (64 bit), **7:** KB3159398, KB3159398 (64 bit), **2008 R2:** KB3159398, **8.1:** KB3159398, KB3159398 (64 bit), **2012:** KB3159398, **2012 R2:** KB3159398.	16-072
Security Update for Microsoft Windows PDF (MS16-080)	Fixes vulnerabilities, of which the more severe could allow remote code execution if a user opens a specially crafted .pdf file. (CVE 2016-3201 CVE 2016-3203 CVE 2016-3215)	**8.1:** KB3157569, KB3157569 (64 bit), **2012:** KB3157569, **2012 R2:** KB3157569.	16-080
Graphics Component Vulnerabilities (MS16-074)	MS16-074 resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow elevation of privilege if a user opens a specially crafted document or visits a specially crafted website using Windows 10. (CVE 2016-3216 CVE 2016-3219)	**Vista:** KB3164035, KB3164035 (64 bit), **2008:** KB3164035, KB3164035 (64 bit), **7:** KB3164035, KB3164035 (64 bit), **2008 R2:** KB3164035 (64 bit), **8.1:** KB3164035, KB3164035 (64 bit), **2012:** KB3164035 (64 bit),	16-074

		2012 R2: KB3164035 (64 bit), **10:** KB3163017, KB3163017 (64 bit).
Graphics Component Elevation of Privilege Vulnerabilities (MS16-074)	MS16-074 resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow elevation of privilege if a user opens a specially crafted document or visits a specially crafted website. (CVE 2016-3219 CVE 2016-3220)	**Vista:** KB3164033, 16-074 KB3164033 (64 bit), **2008:** KB3164033, KB3164033 (64 bit), **7:** KB3164033, KB3164033 (64 bit), **2008 R2:** KB3164033 (64 bit), **8.1:** KB3164033, KB3164033 (64 bit), **2012:** KB3164033 (64 bit), **2012 R2:** KB3164033 (64 bit), **10:** KB3163017, KB3163017 (64 bit).
Multiple Microsoft Graphics Component Vulnerabilities fixed by MS16-146	MS16-146 resolves three vulnerabilities in Microsoft Windows. The two most severe vulnerabilities could allow remote code execution. The third vulnerability could result in information disclosure. (CVE 2016-7257 CVE 2016-7272 CVE 2016-7273)	**Vista:** KB3204724, 16-146 KB3205638, **Server 2008:** KB3204724, KB3205638, **Windows 7:** KB3205394, **Server 2008 R2:** KB3205394, **Windows 8.1:** KB3205400, **Server 2012:** KB3205400, **Server 2012 R2:** KB3205400, **Windows 10:** KB3205383, **Windows 10 Version 1511:** KB3205386 **Windows 10 Version 1607:** KB3206632 **Server 2016:** KB3206632.
Microsoft Video Control Remote Code Execution Vulnerability	MS16-122 remediates a vulnerability that could otherwise allow arbitrary code to be run in the context of the current user. (CVE 2016-0142)	**Vista:** KB3190847, 16-122 KB3190847 (64 bit), **7:** KB3192391,

		KB3185330, KB3192391_(64-bit), KB3185330 (64-bit). **8.1:** KB3192392, KB3185331, KB3192392 (64-bit), KB3185331 (64-bit), **10:** KB3192440, KB3192440 (64 bit).	
Microsoft Windows Secure Boot Security Feature Bypass Vulnerability	MS16-094 resolves a security feature bypass vulnerability in Microsoft Windows Secure Boot caused by improperly applying an affected policy. To exploit this vulnerability, an attacker must either gain administrative privileges or physical access to a target device to install an affected policy. (CVE 2016-3287)	**8.1:** KB3172727, KB3172727 (64 bit) **2012:** KB3172727 (64 bit) **2012 R2:** KB3172727 (64 bit) **10:** KB3163912	16-094
Microsoft Windows Secure Boot Manager Security Feature Bypass Vulnerability	MS16-100 resolves a security feature bypass vulnerability in Microsoft Windows Secure Boot. To exploit this vulnerability, an attacker must either gain administrative privileges or physical access to a target device to install an affected boot manager. (CVE 2016-3320)	**8.1:** KB3172729, KB3172729 (64 bit) **2012:** KB3172729 (64 bit) **2012 R2:** KB3172729 (64 bit) **10:** KB3172729	16-100
Microsoft Windows Secure Boot Manager security feature bypass vulnerability fixed by MS16-140	MS16-140 resolves a security feature bypass vulnerability in Microsoft Windows Secure Boot Manager. To exploit this vulnerability, an attacker must have physical access to a target device to install an affected boot manager. (CVE 2016-7247)	**Windows 8.1:** 3197873 **Server 2012:** 3197876 **Server 2012 R2:** 3197873 **Windows 10:** 3198585 **Windows 10 version 1511:** 3198586 **Windows 10 version 1607:** 3200970 **Server 2016:** 3200970	16-140
Microsoft Windows Search Component Vulnerability (MS16-082)	MS16-082 resolves a vulnerability in Microsoft Windows. The vulnerability could allow denial of service if an attacker logs on to a target system and runs a specially crafted application. (CVE 2016-3230)	**7:** KB3161958, KB3161958 (64 bit), **2008 R2:** KB3161958 (64 bit), **8.1:** KB3161958, KB3161958 (64 bit), **2012:** KB3161958 (64 bit),	16-082

		2012 R2: KB3161958 (64 bit), **10:** KB3163017, KB3163017 (64 bit).	
JScript and VBScript Memory Corruption	Fixes a vulnerability which could allow a malicious web site, application, or document to execute arbitrary code with the privileges of the current user. (CVE 2016-3204)	**Vista:** 3169659 **2008:** 3169659	16-086
Security Update for Windows Print Spooler Components	MS16-087 resolves vulnerabilities in Windows Print Spooler components. The more severe of the vulnerabilities could allow remote code execution if an attacker is able to execute a man-in-the-middle (MiTM) attack on a workstation or print server, or set up a rogue print server on a target network. (CVE 2016-3238 CVE 2016-3239)	**Vista:** KB3170455, KB3170455 (64 bit), **2008:** KB3170455, KB3170455 (64 bit), **7:** KB3170455, KB3170455 (64 bit), **2008 R2:** KB3170455 (64 bit), **8.1:** KB3170455, KB3170455 (64 bit), **2012:** KB3170455 (64 bit), **2012 R2:** KB3170455 (64 bit), **10:** KB3163912, KB3163912 (64 bit).	16-087
Windows Kernel-Mode Win32k Multiple Vulnerabilities (MS16-098)	MS16-098 resolves several elevation of privilege vulnerabilities in Microsoft Windows Kernel-Mode drivers. (CVE 2016-3308 CVE 2016-3309 CVE 2016-3310 CVE 2016-3311)	**Vista:** KB3177725, KB3177725 (64 bit), **2008:** KB3177725, KB3177725 (64 bit), **7:** KB3177725, KB3177725 (64 bit), **2008 R2:** KB3177725, KB3177725 (64 bit), **8.1:** KB3177725, KB3177725 (64 bit), **2012:** KB3177725 (64 bit), **2012 R2:** KB3177725 (64 bit), **10:** KB3176492, **10 Version 1511:** KB3176493, **10 Version 1607:**	16-098

		KB3176495	
Security Update for Microsoft Graphics Component (MS16-106)	MS16-106 resolves multiple vulnerabilities in the Microsoft Graphics Component. The most severe of which could allow elevation of privilege due to the way certain Windows kernel-mode drivers handle objects in memory. (CVE 2016-3348 CVE 2016-3349 CVE 2016-3354 CVE 2016-3355 CVE 2016-3356)	**Vista** KB3185911, KB3185911 (64 bit), **2008:** KB3185911, KB3185911 (64 bit), **7:** KB3185911, KB3185911 (64 bit), **2008 R2:** KB3185911, **8.1:** KB3185911, KB3185911 (64 bit), **2012:** KB3185911, **2012 R2:** KB3185911, **10:** KB3185611, **10 Version 1511:** KB3185614, **10 Version 1607:** KB3189866	16-106
Security Update for SMBv1 (MS16-114)	MS16-114 resolves an issue in SMBv1 that could result in a denial of service condition if leveraged by an attacker. (CVE 2016-3345)	**Vista** KB3177186, KB3177186 (64 bit), **2008:** KB3177186, KB3177186 (64 bit), **7:** KB3177186, KB3177186 (64 bit), **2008 R2:** KB3177186, **8.1:** KB3177186, KB3177186 (64 bit), **2012:** KB3177186, **2012 R2:** KB3177186, **10:** KB3185611, **10 Version 1511:** KB3185614, **10 Version 1607:** KB3189866	16-114
Security Update for Windows Kernel (MS16-111)	MS16-111 resolves multiple elevation of privilege vulnerabilities in Microsoft Windows. (CVE 2016-3305 CVE 2016-3306 CVE 2016-3371 CVE 2016-3372 CVE 2016-3373)	**Vista** KB3175024, KB3175024 (64 bit), **2008:** KB3175024, KB3175024 (64 bit), **7:** KB3175024, KB3175024 (64 bit), **2008 R2:** KB3175024, **8.1:** KB3175024, KB3175024 (64	16-111

		bit), **2012:** KB3175024, **2012 R2:** KB3175024, **10:** KB3185611, **10 Version 1511:** KB3185614, **10 Version 1607:** KB3189866	
Security Update for Windows Login (MS16-112)	MS16-112 resolves a lock screen credential harvesting vulnerability in Microsoft Windows. (CVE 2016-3302)	**8.1:** KB3178539, KB3178539 (64 bit), **2012 R2:** KB3178539, **10:** KB3185611, **10 Version 1511:** KB3185614, **10 Version 1607:** KB3189866	16-112
Security Update for Windows Kernel (MS16-092)	MS16-092 resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow security feature bypass if the Windows kernel fails to determine how a low integrity application can use certain object manager features. (CVE 2016-3258 CVE 2016-3272)	**8.1:** KB3170377, KB3170377 (64 bit), **2012:** KB3170377 (64 bit), **2012 R2:** KB3170377 (64 bit), **10:** KB3163912, KB3163912 (64 bit).	16-092
Microsoft Windows information disclosure vulnerability fixed by MS16-110	MS16-110 patches an information disclosure vulnerability that exists because Windows fails to properly validate NT LAN Manager (NTLM) Single Sign-On (SSO) request during Microsoft Account (MSA) login sessions. The information gleaned by a successful attacker could aid attempts to brute force a user's NTLM password hash. To exploit the vulnerability, an attacker would have to trick a user into one of various actions, such as browsing to a malicious web site. (CVE 2016-3352)	**8.1:** KB3184471, KB3184471 (64 bit), **2012:** KB3184471 (64 bit), **2012 R2:** KB3184471 (64 bit), **10:** KB3185611, KB3185611 (64 bit).	16-110
Microsoft Windows remote code execution vulnerability fixed by MS16-110	MS16-110 patches a remote code execution vulnerability that exists as a result of the way that Windows handles objects in memory. An attacker would need to have a domain user account and then create a specially crafted request that could cause Windows to execute arbitrary code with elevated permissions. (CVE 2016-3368)	**Vista:** KB3184471, KB3184471 (64 bit), **2008:** KB3184471, KB3184471 (64 bit), **7:** KB3184471, KB3184471 (64 bit), **2008 R2:** KB3184471 (64 bit), **8.1:** KB3184471, KB3184471 (64	16-110

		bit), **2012:** KB3184471 (64 bit), **2012 R2:** KB3184471 (64 bit), **10:** KB3185611, KB3185611 (64 bit).	
Two Microsoft Windows 10 vulnerabilities fixed by MS16-110	MS16-110 patches two vulnerabilities in Windows 10. One vulnerability is elevation of privilege due to the way Windows enforces permissions when an attacker loads a specially crafted DLL file. An attacker must be locally authenticated to exploit this vulnerability. The successful attacker could run arbitrary code as a system administrator. A second vulnerability is a denial of service vulnerability that exists as a result of the way Windows handles objects in memory. An attacker who successfully exploits this denial of service vulnerability could prevent authorized users from accessing system resources. (CVE 2016-3346 CVE 2016-3369)	**10:** KB3185611, KB3185611 (64 bit).	16-110
Graphics Component Remote Code Execution Vulnerabilities (MS16-097)	MS16-097 resolves vulnerabilities in Microsoft Windows, Skype for Business, and Microsoft Lync. The vulnerabilities could allow remote code execution if a user either visits a specially crafted website or opens a specially crafted document. (CVE 2016-3301 CVE 2016-3303 CVE 2016-3304)	**Vista:** KB3178034, KB3178034 (64 bit), **2008:** KB3178034, KB3178034 (64 bit), **7:** KB3178034, KB3178034 (64 bit), **2008 R2:** KB3178034 (64 bit), **8.1:** KB3178034, KB3178034 (64 bit), **2012:** KB3178034 (64 bit), **2012 R2:** KB3178034 (64 bit), **10:** KB3176492, KB3176492 (64 bit).	16-097
Microsoft Windows PDF Library Remote Code Execution Vulnerability (MS16-115)	MS16-115 resolves a remote code execution vulnerability in the Windows PDF Library. An attacker that entices a user to open a specially crafted PDF file could reveal information in the context of the current user. (CVE 2016-3370 CVE 2016-3374)	**8.1:** KB3184943, KB3184943 (64 bit), **2012 R2:** KB3184943 (64 bit), **2012:** KB3184943 (64 bit),	16-115

		10: KB3185611, KB3185611 (64 bit).	
Windows Secure Kernel Mode Information Disclosure Vulnerability	Fixes an information disclosure vulnerability which could be exploited by a local authenticated user. (CVE 2016-3344)	**10**: 3185611 **10 Version 1511**: 3185614	16-113
SharePoint Server and Office Web Apps memory corruption vulnerabilities	Fixes multiple vulnerabilities which could allow command execution when a user opens a specially crafted file. (CVE 2016-3357 CVE 2016-3358 CVE 2016-3360 CVE 2016-3362 CVE 2016-3365)	**Excel Services on Microsoft SharePoint Server 2007**: 3115112 **Excel Services on Microsoft SharePoint Server 2010**: 3115119 **Word Automation Services on Microsoft SharePoint Server 2010**: 3115466 **Microsoft SharePoint Server 2013**: 3054862 **Excel Automation Services on Microsoft SharePoint Server 2013**: 3115169 **Word Automation Services on Microsoft SharePoint Server 2013**: 3115443 **Microsoft Office Web Apps 2010**: 3115472 **Microsoft Office Web Apps Server 2013**: 3118270 **Office Online Server**: 3118299	16-107
Scripting Engine Memory Corruption Vulnerability (MS16-116)	MS16-116 resolves a vulnerability in conjunction with the IE update in MS16-104, addresses the vulnerability by modifying how the Microsoft OLE Automation mechanism and the VBScript Scripting Engine in Internet Explorer handle objects in memory. (CVE 2016-3375)	**Vista:** KB3184122, KB3184122 (64 bit), **2008:** KB3184122, KB3184122 (64 bit), **7:** KB3184122, KB3184122 (64 bit), **2008 R2:** KB3184122 (64	16-116

		bit), **8.1:** KB3184122, KB3184122 (64 bit), **2012:** KB3184122 (64 bit), **2012 R2:** KB3184122 (64 bit), **10:** KB3185611, KB3185611 (64 bit).	
Microsoft Video Control Remote Code Execution Vulnerability	Fixes a remote code execution vulnerability in the Microsoft Video Control. (CVE 2016-7248)	**Vista**: 3198218 **Windows 7**: 3197868 **Windows 8.1**: 3197874 **Windows 10**: 3198585 **Windows 10 version 1511**: 3198586 **Windows 10 version 1607**: 3200970	16-131
Windows Kernel Elevation of Privilege Vulnerability	Fixes a local Windows kernel elevation of privilege vulnerability that could be triggered by a malicious application. (CVE 2016-7216)	**Vista**: 3198483 **Windows Server 2008**: 3198483 **Windows 7**: 3197867 **Windows Server 2008 R2**: 3197867	16-139
Windows Diagnostics Hub Elevation of Privilege	Fixes an insecure library loading vulnerability in the Windows Diagnostics Hub Standard Collector Service. (CVE 2016-7188)	**10**: 3192440 **10 Version 1511**: 3192441 **10 Version 1607**: 3194798	16-125
Security Update for Microsoft Graphics Component (MS16-120)	Fixes information disclosure, elevation of privilege, and remote code execution vulnerabilities when the Windows GDI component fails to properly handle objects in memory. These vulnerabilities also affected Skype for Business 2016, Microsoft Lync, and Microsoft Live Meeting. (CVE 2016-3209 CVE 2016-3262 CVE 2016-3263 CVE 2016-3270 CVE 2016-3393 CVE 2016-3396 CVE 2016-7182)	**Windows Vista:** 3191203, 3191203 (64-bit), **Windows 2008:** 3191203, 3191203 (64-bit), **Windows 7:** 3192391, 3192391 (64-bit), 3185330, 3185330 (64-bit), **Windows 2008 R2:** 3192391, 3185330, **Windows 8.1:** 3192392, 3192392 (64-bit), 3185331, 3185331 (64-bit), **Windows 2012:** 3192393, 3185332, **Windows 2012**	16-120

		R2: 3192392, 3185331 (64-bit), **Windows 10:** 3192440, Version 1511 (3192441), Version 1607 (3194798), **Skype for Business 2016:** 3118327, 3118327 (64-bit), **Microsoft Lync 2013:** 3118348, 3118348 (64-bit), **Microsoft Lync 2010:** 3188397, 3188397 (64-bit), **Microsoft Live Meeting 2007:** 3189647.	
LSASS Denial of Service vulnerability (MS17-004)	Resolves a denial of service vulnerability in the Windows LSASS Service that could be exploited by an attacker. A successful attack causes the victim machine to reboot. (CVE 2017-0004)	**Windows Vista:** 3216775 **Windows Server 2008:** 3216775 **Windows 7:** 3212642 **Windows Server 2008 R2:** 3212642	17-004
Security Update for Microsoft Windows (MS16-149)	Resolves an elevation of privilege vulnerability in the Windows Installer and an information disclosure vulnerability in Windows Crypto Driver. (CVE 2016-7219 CVE 2016-7292)	**Windows Vista:** 3204808, 3196726 **Windows Server 2008:** 3204808, 3196726 **Windows 7:** 3205394 **Windows Server 2008 R2:** 3205394 **Windows 8.1:** 3205400 **Windows Server 2012:** 3205408 **Windows Server 2012 R2:** 3205400 **Windows 10:** 3205383 **Windows 10 Version 1511:** 3205386 **Windows 10 Version 1607:** 3206632 **Windows 2016** 3206632	16-149
Security Update for Windows Kernel-Mode Drivers (MS16-151)	Resolves multiple Windows Kernel-Mode Driver vulnerabilities that	**Windows Vista:** 3204723	16-151

	could potentially allow elevation of privilege. (CVE 2016-7259 CVE 2016-7260)	**Windows Server 2008:** 3204723 **Windows 7:** 3205394 **Windows Server 2008 R2:** 3205394 **Windows 8.1:** 3205400 **Windows Server 2012:** 3205408 **Windows Server 2012 R2:** 3205400 **Windows 10:** 3205383 **Windows 10 Version 1511:** 3205386 **Windows 10 Version 1607:** 3206632 **Windows 2016:** 3206632	
Security Update for Windows Kernel-Mode Drivers (MS16-135)	Resolves multiple Windows Kernel-Mode Driver vulnerabilities that could potentially allow elevation of privilege. (CVE 2016-7214 CVE 2016-7215 CVE 2016-7218 CVE 2016-7246 CVE 2016-7255)	**Windows Vista:** 3198234, 3198234 (64 bit), 3194371, 3194371 (64 bit), **Windows Server 2008:** 3198234, 3198234 (64 bit), 3194371, 3194371 (64 bit), **Windows 7:** 3197867, 3197868, 3197867 (64 bit), 3197868 (64 bit), **Windows Server 2008 R2:** 3197867, 3197868, **Windows 8.1:** 3197873, 3197873 (64 bit), **Windows Server 2012:** 3197876, 3197877, **Windows Server 2012 R2:** 3197873, **Windows 10:** 3198585, 3198585 (64 bit), **Windows 2016:** 3200970.	16-135
Security Update for Windows Kernel-Mode Drivers (MS16-123)	Fixes elevation of privilege vulnerabilities when the Windows	**Windows Vista:** 3191203, 3191203	16-123

	kernel-mode driver fails to properly handle objects in memory. (CVE 2016-3266 CVE 2016-3341 CVE 2016-3376 CVE 2016-7185 CVE 2016-7211)	(64 bit), 3183431, 3183431 (64 bit), **Windows Server 2008:** 3191203, 3191203 (64 bit), 3183431, 3183431 (64 bit), **Windows 7:** 3192391, 3192391 (64 bit), 3185330, 3185330 (64 bit), **Windows Server 2008 R2:** 3192391, 3185330, **Windows 8.1:** 3192392, 3192392 (64 bit), 3185331, 3185331 (64 bit), **Windows Server 2012:** 3192393, 3185332, **Windows Server 2012 R2:** 3192392, 3185331, **Windows 10:** 3192440, Version 1511 (3192441), Version 1607 (3194798).	
Windows Common Log File System elevation of privilege vulnerabilities fixed by MS16-134	Fixes elevation of privilege vulnerabilities when the Windows Common Log File System driver fails to properly handle objects in memory. (CVE 2016-0026 CVE 2016-3332 CVE 2016-3333 CVE 2016-3334 CVE 2016-3335 CVE 2016-3338 CVE 2016-3340 CVE 2016-3342 CVE 2016-3343 CVE 2016-3384)	**Vista:** 3181707 **Server 2008:** 3181707 **Windows 7:** 3197867 **Server 2008 R2:** 3197867 **Server 2012:** 3197876 **Windows 8.1:** 3197873 **Server 2012 R2:** 3197873 **Windows 10:** 3198585 **Windows 10 version 1511:** 3198586 **Windows 10 version 1607:** 3200970 **Server 2016:** 3200970	16-134
Windows Common Log File System information disclosure vulnerability fixed by MS16-153	Fixes an information disclosure vulnerability when the Windows Common Log File System driver fails to properly handle objects in memory.	**Vista:** KB3203838 **Server 2008:** KB3203838 **Windows 7:**	16-153

	(CVE 2016-7295)	KB3205394 **Server 2008 R2:** KB3205394 **Server 2012:** KB3205408 **Windows 8.1:** KB3205400 **Server 2012 R2:** KB3205400 **Windows 10:** KB3205383, **Windows 10 Version 1511:** KB3205386 **Windows10 Version 1607:** KB3206632 **Server 2016:** KB3206632.	
Microsoft Graphics Component vulnerabilities	Fixes vulnerabilities in Open Type fonts, Windows Animation Manager, and Media Foundation. (CVE 2016-7205 CVE 2016-7210 CVE 2016-7217 CVE 2016-7256)	**Vista**: 3203859 **2008**: 3203859 **7**: 3197868 **2008 R2**: 3197868 **8.1**: 3197874 **2012**: 3197877 **2012 R2**: 3197874 **10**: 3198585 **10 Version 1511**: 3198586 **10 Version 1607**: 3200970 **2016**: 3200970	16-132
Microsoft Virtual Hard Disk Driver privilege elevation	Fixes a vulnerability which could allow a user on the local system to manipulate files which should be protected. (CVE 2016-7223 CVE 2016-7224 CVE 2016-7225 CVE 2016-7226)	**8.1**: 3197874 **2012**: 3197877 **2012 R2**: 3197874 **10**: 3198585 **10 Version 1511**: 3198586 **10 Version 1607**: 3200970 **2016**: 3200970	16-138
Security Update for Microsoft Windows (MS16-130)	Fixes three vulnerabilities, of which the most severe could allow remote code execution. (CVE 2016-7212 CVE 2016-7221 CVE 2016-7222)	**Vista**: 3193418 **2008**: 3193418 **7**: 3197867 **2008 R2**: 3197867 **8.1**: 3197873 **2012**: 3197876 **2012 R2**: 3197873 **10**: 3198585 **10 Version 1511**: 3198586 **10 Version 1607**: 3200970 **2016**: 3200970	16-130
Security Update for Windows Authentication Methods (MS16-137)	Fixes three vulnerabilities, of which the most severe could allow elevation of privilege. (CVE 2016-7220 CVE 2016-7237 CVE 2016-7238)	**Vista**: 3198510 **2008**: 3198510 **7**: 3197867 **2008 R2**: 3197867	16-137

		8.1: 3197873 **2012**: 3197873 **2012 R2**: 3197873 **10**: 3198585 **10 Version 1511**: 3198586 **10 Version 1607**: 3200970 **2016**: 3200970	
Windows Kernel Memory Information information disclosure	Fixes a flaw in the Windows kernel's handling of certain page fault system calls which could allow an authenticated attacker to disclose information from one process to another. (CVE 2016-7258)	**10**: 3205383 **10 Version 1511**: 3205386 **10 Version 1607**: 3206632 **2016**: 3206632	16-152
Microsoft Windows Communications Platforms and Software Vulnerabilities (June 2017)	The June 2017 update fixes a vulnerability in Skype for Business 2016 and Lync Server 2010 and 2013. The vulnerability could lead to remote code execution. (CVE 2017-0283 (CVE 2017-8527)	**Skype for Business 2016**: 3203382 3203382 (64 Bit) **Microsoft Lync 2013**: 3191939 3191939 (64 Bit) **Microsoft Lync 2010**: 4020732 4020732 (64 Bit)	KB3191858
Microsoft Windows Communications Platforms and Software Vulnerabilities (Sept 2017)	The Sept 2017 update fixes vulnerabilities in Skype for Business 2016, Lync Server 2010, Lync 2013 and Live Meeting 2007. These vulnerabilities could allow information disclosure or lead to remote code execution. (CVE 2017-8676 CVE 2017-8695 CVE 2017-8696)	**Skype for Business 2016**: 4011040 4011040 (64 Bit) **Microsoft Lync 2013**: 4011107 3213568 4011107 (64 Bit) 3213568 (64 Bit) **Microsoft Lync 2010**: 4025865 4025865 (64 Bit) **Lync 2010 Attendee User Level**: 4025867 **Lync 2010 Attendee Admin Level**: 4025866 **Live Meeting 2007**: 4025868 4025869	KB4011040
Security Update for Skype for Business 2016 and Lync 2013	The October 2017 fixes an elevation of privilege vulnerability in Skype for Business 2016 and Lync 2013. The vulnerability could allow an authenticated attacker to steal an authentication hash that can be reused elsewhere. (CVE 2017-11786)	**Microsoft Lync 2013**: 4011179 4011179 (64 Bit) **Skype for Business 2016**: 4011159 4011159 (64 Bit)	KB4011179 and KB4011159
Microsoft Windows Communications Platforms and Software Vulnerabilities (May 2017)	The May 2017 update fixes a vulnerability in Skype for Business 2016. The vulnerability could lead to remote code execution. (CVE 2017-0281)	**Skype for Business 2016**: 3191858 3191858 (64 Bit)	KB3191858

Microsoft Windows Communications Platforms and Software Vulnerabilities (MS17-013)	MS17-013 fixes several vulnerabilities in the graphics components of Skype for Business 2016, Lync 2010, Lync 2013, and Live Meeting 2007. The most severe of these vulnerabilities could lead to remote code execution. (CVE 2017-0060 CVE 2017-0073 CVE 2017-0108)	**Skype for Business 2016**: 3178656 3178656 (64-bit) **Lync 2013 (Skype for Business 2015)**: 3172539 3172539 (64-bit) **Lync 2010**: 4010299 4010299 (64-bit) **Lync 2010 Attendee User Level**: 4010300 **Lync 2010 Attendee Admin Level**: 4010301 **Live Meeting 2007**: Conferencing Add-in for Microsoft Office Outlook	17-013
Windows Secure Kernel Mode Elevation of Privilege	Fixes a vulnerability by correcting how Windows handles objects in memory to properly enforce virtual trust levels. (CVE 2016-7271)	**Windows 10**: 3205383 **Windows 10 Version 1511**: 3205386 **Windows 10 Version 1607**: 3206632 **Server 2016**: 3206632	16-150
Windows Uniscribe Remote Code Execution Vulnerability (MS16-147)	The security update addresses two vulnerabilities by correcting how the Windows Uniscribe handles objects in the memory. (CVE 2016-7274)	**Windows Vista:** 3196348 **Windows Server 2008:** 3196348 **Windows 7:** 3205394 3207752 **Windows Server 2008 R2:** 3205394 3207752 **Windows 8.1:** 3205400 3205401 3205400(64 bit) **Windows 10:** 3205383 **Windows 10 Version 1511:** 3205386 **Windows 10 Version 1607:** 3206632 **Windows Server 2012:** 3205408 3205409 **Windows Server**	16-147

		2012 R2: 3205400 3205401 **Windows 2016:** 3206632	
Windows olecnv32.dll Remote Code Execution Vulnerability	Fixes a vulnerability which could allow remote code execution. (CVE 2017-8487)	**Windows XP and 2003:** 4025218	CVE-2017-8487
Windows RPC Remote Code Execution Vulnerability	Windows RPC with Routing and Remote Access enabled in Windows XP and Windows Server 2003 allows an attacker to execute code on a targeted RPC server. (CVE 2017-8461)	**Windows XP and 2003:** 4024323	CVE-2017-8461
Remote Desktop Protocol Remote Code Execution Vulnerability	Fixed a buffer overflow in Smart Card authentication code in gpkcsp.dll which allows a remote attacker to execute arbitrary code on the target computer. (CVE 2017-0176)	**Windows XP and 2003:** 4022747	CVE-2017-0176
Windows (MS15-097) vulnerable version, secdrv.sys	MS15-097 security bulletin addresses a defense-in-depth update for the secdrv.sys driver, a third-party driver. (CVE 2018-7249 CVE 2018-7250)	**Windows Vista:** KB3086255 KB3086255 (64 bit) **Windows 7:** KB3086255 KB3086255 (64 bit) **Windows 8:** KB3086255 KB3086255 (64 bit) **Windows 8.1:** KB3086255 KB3086255 (64 bit)	MS15-097
Microsoft Skype for Business 2016 and Lync 2013 remote code execution (July 2018)	The July 2018 security update fixed two vulnerabilities in Microsoft Skype for Business 2016 and Lync 2013 (Skype for Business 2015) including a security bypass vulnerability and remote code execution vulnerability. (CVE 2018-8238, CVE 2018-8311)	**Skype for Business 2016 (64-bit)**:KB4022221 **Skype for Business 2016 (32-bit)**:KB4022221 **Lync 2013 - Skype for Business 2015 (64-bit)**:KB4022225 **Lync 2013 - Skype for Business 2015 (32-bit)**:KB4022225	KB4022221 and KB4022225
Microsoft SharePoint 2013 remote code execution (July 2018)	The July 2018 security update fixed several vulnerabilities in Microsoft SharePoint 2013 including an elevation of privilege vulnerability and remote code execution vulnerability. (CVE 2018-8299, CVE 2018-8300, CVE	**SharePoint Foundation 2013**:KB4022243 **SharePoint Enterprise 2013**:KB4022235	KB4022243 and KB4022235

	2018-8323)		
Microsoft SharePoint Server 2010 Excel Services Elevation of Privilege (Dec 2018)	The December 2018 security update fixed an elevation of privilege vulnerability in Microsoft SharePoint Server 2010 Excel Services. (CVE 2018-8627)	**Microsoft SharePoint Server 2010 Excel Services**: KB4461569	KB4461569
Microsoft Skype for Business 2016 and Lync 2013 denial of service (Nov 2018)	The Nov 2018 security update fixed a DOS vulnerability in Microsoft Skype for Business 2016 and Lync 2013. (CVE 2018-8546)	**Skype for Business 2016 (64-bit)**:KB4461473 **Skype for Business 2016 (32-bit)**:KB4461473 **Lync 2013 (64-bit)**:KB4461487 **Lync 2013 (32-bit)**:KB4461487	KB4461473 and KB4461487
Microsoft Lync Server 2013 cross-site scripting (March 2019)	The March 2019 update for Lync 2013 fixed a spoofing vulnerability. (CVE 2019-0624 CVE 2019-0798)	**Lync Server 2013 Cumulative Update**: KB2809243	KB2809243
Microsoft Lync Server 2010 and 2013 denial of service (June 2019)	The June 2019 update for Lync Server 2010 and 2013 fixed a denial of service vulnerability. (CVE 2019-1029)	**Lync Server 2010 Cumulative Update**: KB2493736 **Lync Server 2013 Cumulative Update**: KB2809243	KB4506009
Microsoft Lync 2013 information disclosure (September 2019)	The September 2019 update for Lync 2013 fixed a vulnerability which could allow an attacker to read arbitrary files after a user follows a specially crafted meeting link. (CVE 2019-1209)	**Lync 2013 Cumulative Update**: 2809243	CVE-2019-1209

Scan Session: ElectricbirdContoso Full Scan_FUl44G; Scan Policy: heavy vulnerability; Scan Data Set: 7 January 2022 01:15