EventTracker
Secure. Comply. Succeed.

Detecting and Patching FREAK Vulnerability (CVE-2015-0204)

EventTracker v7.x

Whitepaper
Publication Date: Mar 17, 2015

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This document provides Information about **FREAK Vulnerability (CVE-2015-0204)** recently discovered on *nix based Operating Systems and devices running OpenSSL versions before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k. Systems running Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8 and Windows 8.1, Windows Server 2012 and Windows Server 2012 R2, Windows RT and Windows RT 8.1, windows 2008, 2008 R2, Windows 2012 and 2012 R2 Server Core installation are affected.

This document also provides guidance to the user about detecting this threat using **EventTracker Vulnerability Assessment Service (ETVAS)** and **EventTracker Intrusion Detection Service (ETIDS)** and how to patch the vulnerable servers.

EventTracker with **ETIDS** and **ETVAS** can be used to detect FREAK vulnerability in the Network.

Scope

The configurations detailed in this guide are consistent with EventTracker 7.0, **ETIDS** and **ETVAS.**

Target Audience

IT administrators or Security administrators who are responsible for maintaining security for the IT infrastructure.

Table of Contents

Introduction

A newly discovered vulnerability in the SSL and TLS cryptographic protocols could allow attackers to intercept and decrypt communications between affected clients and servers. Dubbed the 'FREAK" vulnerability, it facilitates man-in-the-middle (MITM) attacks against secure connections where the server accepts RSA_EXPORT cipher suites and the client either offers an RSA_EXPORT suite or uses an older, unpatched version of OpenSSL. Once the encryption is broken by the attackers, they could steal passwords and other personal information and potentially launch further attacks against the website.

Microsoft revealed that the vulnerability did affect Microsoft products and existed in Secure Channel (Schannel), a security package that implements the SSL/TLS protocols. Using the vulnerability, a man-in-the-middle attacker could downgrade the key length of a RSA key to EXPORT-grade length in a TLS connection and decipher communications. Any Windows system using Schannel to connect to a remote TLS server with an insecure cipher suite is affected.

EventTracker with ETIDS and ETVAS deployed in network can be easily automated to detect FREAK exploitation and report for the vulnerable devices.

Affected operating systems

- Linux OS running OpenSSL,
- Windows OS.

Identify the vulnerable systems/devices in your network.

Detecting FREAK Exploit attempt using EventTracker and ETIDS.

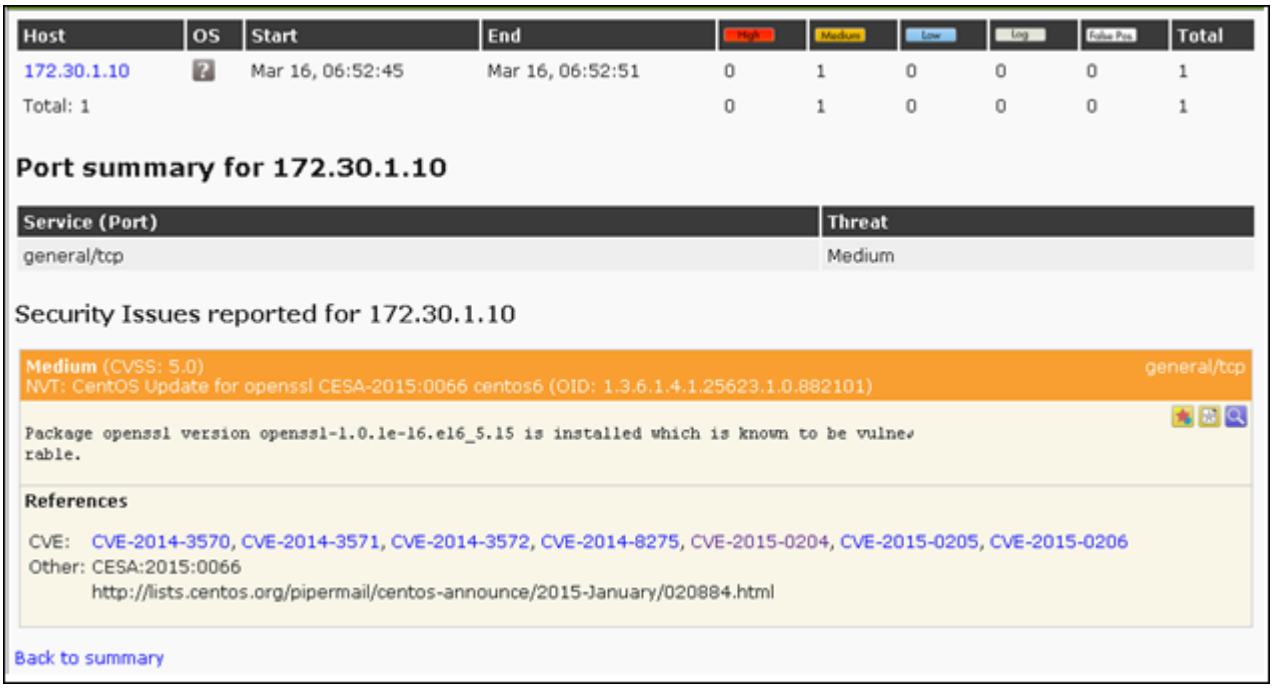
If ETIDS is deployed in enterprise and it sees all the traffic passing to and from critical servers, then it forwards IDS alerts to EventTracker and the alerts, reports are generated, if any of such exploit attempts detected.

For ETIDS configured to use Snort VRT rules EventTracker SNORT IDS alert and report will have alert message listed as '**SSL request for export grade cipher suite attempt"**

For ETIDS configured to use Emerging Threat open rules for snort, EventTracker IDS alert and report will have alert message listed as '**ET EXPLOIT FREAK Weak Export Suite from Server (CVE-2015-0204)".**

Detecting Vulnerable Systems using EventTracker Vulnerability Assessment Service (ETVAS).

EventTracker provides ETVAS as virtual appliance which is easily deployed and configured to scan network and it provides report for vulnerable systems which is running vulnerable version of OpenSSL. Below is the sample report.



Host	OS	Start	End	High	Medium	Low	Log	False Pos	Total
172.30.1.10		Mar 16, 06:52:45	Mar 16, 06:52:51	0	1	0	0	0	1
Total: 1				0	1	0	0	0	1

Port summary for 172.30.1.10

Service (Port)	Threat
general/tcp	Medium

Security Issues reported for 172.30.1.10

Medium (CVSS: 5.0) general/tcp
NVT: CentOS Update for openssl CESA-2015:0066 centos6 (OID: 1.3.6.1.4.1.25623.1.0.882101)

Package openssl version openssl-1.0.1e-16.el6_5.15 is installed which is known to be vulnerable.

References

CVE: CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206
Other: CESA:2015:0066
http://lists.centos.org/pipermail/centos-announce/2015-January/020884.html

Back to summary

Figure 1

Protecting systems by patching your vulnerable systems

Ubuntu/Debian

For currently supported versions of Ubuntu or Debian, update Bash to the latest version available via apt-get:

```
sudo apt-get update && sudo apt-get install --only-upgrade openssl
```

CentOS / Red Hat / Fedora

sudo yum update openssl

Other devices running OpenSSL

Contact Device vendor to know whether these devices are vulnerable and how to patch the device.

Mitigation

Linux Servers

To mitigate the vulnerability described in this Document, you may also disable EXPORT-grade ciphers in your client or server. Doing so, on the server is recommended, especially when you cannot ensure that all clients connecting to your server have been patched.

Disabling EXPORT ciphers on the command line

OpenSSL allows for explicit disabling of EXPORT-grade ciphers by specifying a custom cipher string. For example, when invoking it on the command line, use:

openssl ciphers MEDIUM

Disabling EXPORT ciphers in httpd

To disallow the use of EXPORT-grade ciphers by the httpd web server, add the !EXP directive to the SSLCipherSuite line in the /etc/httpd/conf.d/ssl.conf configuration file. For example:

SSLCipherSuite HIGH:!aNULL:!MD5:!EXP

Restarting Processes for the Changes to Take Effect

The safest and simplest course of action is to perform a full system reboot.

Windows systems

Windows systems running Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8 and Windows 8.1, Windows Server 2012 and Windows Server 2012 R2, Windows RT and Windows RT 8.1, windows 2008, 2008 R2, Windows 2012 and 2012 R2 Server Core installation are affected.

Microsoft has released Security Bulletin MS15-031 which resolves a vulnerability in Microsoft Windows that facilitates exploitation of the publicly disclosed FREAK technique, an industry-wide issue that is not specific to Windows operating systems.

Make sure you have applied updates available in
link https://technet.microsoft.com/library/security/MS15-031 on windows OS.

References:-

https://technet.microsoft.com/library/security/MS15-031

https://www.openssl.org/news/secadv_20150108.txt (look for CVE-2015-0204)

https://www.ssllabs.com/ssltest/viewMyClient.html (Test your browser for SSL vulnerability)

https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp(Check your certificate installation)