tenable® network security

OpenSSL Vulnerabilities Announced on June 5, 2014

How Does It Affect You?

Overview

Several new vulnerabilities related to OpenSSL were disclosed on 6/5/14. Of these, the most serious is **CVE-2014-0224**. It deals with how OpenSSL handles the 'ChangeCipherSpec' message in the SSL protocol, tricking the client and server to communicate without encryption. And, unlike Heartbleed, which penalizes organizations running on the latest release, CVE-2014-0224 affects a broader set of OpenSSL systems.

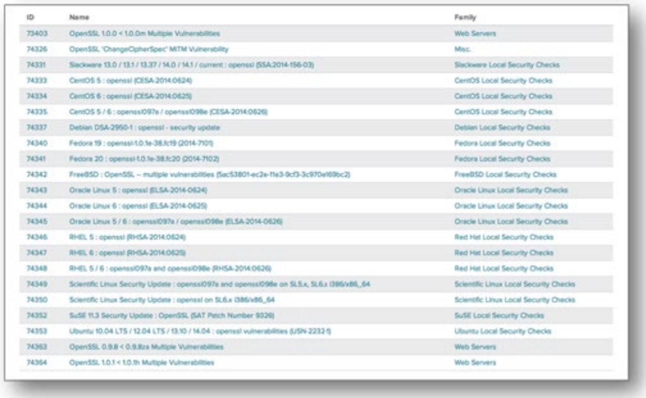
By comparison, exploiting this vulnerability is more complex and the attack is much more targeted than Heartbleed. In order to take advantage of this vulnerability, the attacker needs to launch a man-in-the-middle attack. To exploit, both ends of the conversation need to be vulnerable; fixing just the web browser fixes the issue for example. This vulnerability complements existing man-in-the-middle attacks that exploit weak SSL already (such as hoping a user accepts an incorrect SSL certificate). Organizations of all sizes are concerned about the recent surge in vulnerabilities related to OpenSSL and CVE-2014-0224 is yet another vulnerability that may erode confidence in the security of the "cloud."

How can Tenable help you?

Tenable has released several new updates for multiple products including Nessus® and the Passive Vulnerability Scanner™ that will help customers detect this vulnerability:

Question	Response
Name of Threat	• OpenSSL Security Advisory [05 Jun 2014] • CVE-2014-0224 – MiTM vulnerability • CVE- 2014-0195 – was published and covers a DoS and potential code execution vulnerability (separate from the MiTM attack). Nessus contains plugins to check for this CVE as well.
What is it?	An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server.
Who is affected?	Both the client and server must be vulnerable for the attack to be successful. • Clients: OpenSSL clients in all versions of OpenSSL • Servers: OpenSSL 1.0.1 and 1.0.2-beta1 servers. Users of OpenSSL servers earlier than 1.0.1 are advised to upgrade as a precaution NOTE: Most widely deployed web browsers (for example IE, Google Chrome, Mozilla Firefox, Safari) on desktops are NOT vulnerable as they are not using the OpenSSL libraries. However, Chrome for Android does use OpenSSL, and Google has released an updated version which fixes the vulnerability.
How serious is the issue?	While this vulnerability is not as critical as Heartbleed, it is definitely serious. It requires several conditions to be exploited: the client and the server must use OpenSSL, which excludes most web browsers already (but not VPN clients), and the attacker must be able to sniff the traffic, which also greatly reduces the exposure of the attack.
What is the workaround/fix?	No patch is available. The workaround for this is to upgrade to the latest versions of OpenSSL: • OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za • OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m • OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h
Does an exploit already exist?	Unknown at this time.
Which Tenable products detect the vulnerability?	• Nessus and Nessus Enterprise - Plugin#74326. An updated version of the Nessus UI will be pushed alongside the plugin. It modifies the "Heartbleed" detection wizard to also enable plugin#74326 • Nessus and Nessus Enterprise – Several local checks have been released for Linux and UNIX distributions and specific checks for web servers implementing vulnerable OpenSSL libraries • Nessus Enterprise Cloud – already updated with the new plugin • SecurityCenter™ - plugin#74326 as soon as it hits the feed • SecurityCenter CV™ - plugin#74326 and PVS 8253 as soon as it hits the feed • Passive Vulnerability Scanner (PVS) – plugin 8253 was also added to detect OpenSSL
How does a customer find out if they are susceptible?	Customers must scan their environments, using both remote and local checks, to find out if their environments are susceptible to this vulnerability. Currently any Tenable solution that includes Nessus can be used to identify the vulnerability.

Question	Response
What are the details for scanning for this?	Detailed steps can be found here. http://www.tenable.com/blog/detect-the-latest-openssl-vulnerabilities-using-active-and-passive-scanning And even more details can be found here: https://discussions.nessus.org/message/26183#26183
How do I download the plugin for detection?	New plugins will be downloaded automatically, provided this feature is enabled (the default configuration) and has Internet access, for all product families (Nessus, Nessus Enterprise, PVS and SecurityCenter CV). For Nessus Enterprise Cloud, customers will receive the updates automatically without taking any action.
What can you do if you detect the vulnerability?	You must upgrade to the latest version of OpenSSL. • OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za • OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m • OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h
What can you do to prevent exposure?	Upgrade your OpenSSL per above.
How can customers monitor ongoing exposure?	A regular scan of your environment can help identify if you are vulnerable and identify the issue. Customers that have deployed multiple Nessus scanners and are interested in continuously monitoring for OpenSSL vulnerabilities should evaluate SecurityCenter Continuous View, which incorporates additional technologies like the Passive Vulnerability Scanner (PVS) and Log Correlation Engine (LCE), in addition to Nessus active vulnerability scanning, to offer real-time vulnerability and threat assessment and automatically deliver the latest dashboard (Figure 1 below) and reports. For more information, please read this blog. http://www.tenable.com/sc-dashboards/openssl-changecipherspec-dashboard To evaluate SecurityCenter, please click here
Resources	Good (somewhat technical) presentation from SANS: https://isc.sans.edu/diaryimages/openssljune5th2014.pdf



ID	Name	Family
73403	OpenSSL 1.0.0 < 1.0.0m Multiple Vulnerabilities	Web Servers
74326	OpenSSL 'ChangeCipherSpec' MITM Vulnerability	Misc.
74331	Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssl (SSA:2014-156-03)	Slackware Local Security Checks
74333	CentOS 5 : openssl (CESA-2014:0624)	CentOS Local Security Checks
74334	CentOS 6 : openssl (CESA-2014:0625)	CentOS Local Security Checks
74335	CentOS 5 / 6 : openssl097a / openssl098e (CESA-2014:0626)	CentOS Local Security Checks
74337	Debian DSA-2950-1 : openssl - security update	Debian Local Security Checks
74340	Fedora 19 : openssl-1.0.1e-38.fc19 (2014-7101)	Fedora Local Security Checks
74341	Fedora 20 : openssl-1.0.1e-38.fc20 (2014-7102)	Fedora Local Security Checks
74342	FreeBSD : OpenSSL -- multiple vulnerabilities (5ac53801-ec2e-11e3-9cf3-3c970e169bc2)	FreeBSD Local Security Checks
74343	Oracle Linux 5 : openssl (ELSA-2014-0624)	Oracle Linux Local Security Checks
74344	Oracle Linux 6 : openssl (ELSA-2014-0625)	Oracle Linux Local Security Checks
74345	Oracle Linux 5 / 6 : openssl097a / openssl098e (ELSA-2014-0626)	Oracle Linux Local Security Checks
74346	RHEL 5 : openssl (RHSA-2014:0624)	Red Hat Local Security Checks
74347	RHEL 6 : openssl (RHSA-2014:0625)	Red Hat Local Security Checks
74348	RHEL 5 / 6 : openssl097a and openssl098e (RHSA-2014:0626)	Red Hat Local Security Checks
74349	Scientific Linux Security Update : openssl097a and openssl098e on SL5.x, SL6.x i386/x86_64	Scientific Linux Local Security Checks
74350	Scientific Linux Security Update : openssl on SL6.x i386/x86_64	Scientific Linux Local Security Checks
74352	SuSE 11.3 Security Update : OpenSSL (SAT Patch Number 9326)	SuSE Local Security Checks
74353	Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 : openssl vulnerabilities (USN-2232-1)	Ubuntu Local Security Checks
74363	OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities	Web Servers
74364	OpenSSL 1.0.1 < 1.0.1h Multiple Vulnerabilities	Web Servers

Figure 1: Plugins for CVE-2014-0224 as of June6, 2014 4:30PM EST

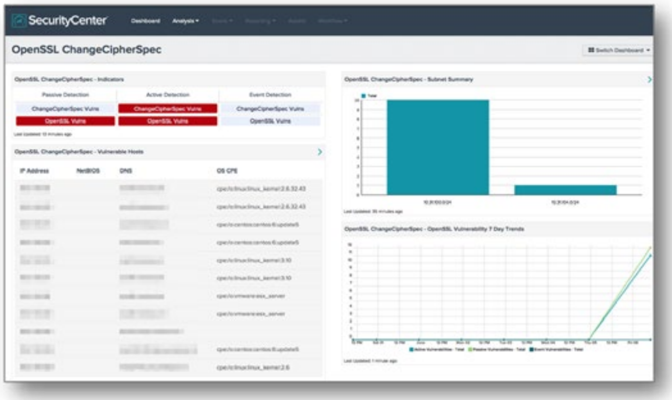


Figure 2: SecurityCenter Dashboard for OpenSSL Vulnerabilities

This dashboard identifies systems vulnerable to the new OpenSSL ChangeCipherSpec vulnerability. The dashboard and its components are available in the SecurityCenter Feed, an app store of dashboards, reports, and assets. The dashboard can be easily located in the SecurityCenter Feed by selecting the category called Security Industry Trends, and then selecting tags SSL and Vulnerabilities.

This dashboard provides SecurityCenter customers with a good summary of the new vulnerabilities recently discovered within OpenSSL. There are six CVEs related to this new vulnerability. This dashboard contains four components, three of which focus on the six CVEs related to the OpenSSL ChangeCipherSpec vulnerability. The remaining component focuses on OpenSSL vulnerabilities.

For More Information

Questions, purchasing, or evaluation:
partnersamer@tenable.com or 443-545-2103
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable®
network security