Heartbleed (CVE-2014-0160) Compensating Controls

Technical Summary

A critical vulnerability in OpenSSL (CVE-2014-0160: OpenSSL Private Key Disclosure Vulnerability) was recently disclosed, affecting servers running OpenSSL 1.0.1 through 1.0.1f. This vulnerability allows arbitrary memory readout, which effectively exposes primary key material and compromises the integrity of the secure channel.

For additional information, please see the Heartbleed Bug Advisory.

Vendor Compensating Controls

Palo Alto Networks

Partner Reference: 36416

Published: 4/9/2014

Protection provided by: PANOS 3.1.0 or above

Protection Overview:

This protection will detect and block attempts to exploit this vulnerability. In order for the protection to be activated, Palo Alto Networks customers with a Threat Prevention subscription are advised to verify that they are running the latest content version on their devices. The threat content version number, including this protection, is 429 or above.

How Can I Protect My Network?

Install the latest threat content, version 429 or above, and ensure that you are using threat prevention for all SSL traffic.

How Do I Know if My Network is Under Attack?

Threat Log and Application Control will show signature ID 36416.

Check Point

Partner Reference: CPAI-2014-1336

Published: 4/9/2014

Protection provided by: R75 or above Security Gateway with IPS

Protection Overview:

This protection will detect and block attempts to exploit this vulnerability. In order for the protection to be activated, update your Security Gateway product to the latest IPS update.

How Can I Protect My Network?

- In the IPS tab, click Protections. Find the OpenSSL TLS DTLS Heartbeat Information Disclosure protection using the Search tool and edit the protection's settings.
- Install policy on all modules.

How Do I Know if My Network is Under Attack?

SmartView Tracker will log the following entries:

- Attack Name: SSL Enforcement Violation
- Attack Information: OpenSSL TLS DTLS Heartbeat Information Disclosure

McAfee Network Security Platform

Partner Reference: KB55447

Published: 04/08/2014

Protection provided by:

- McAfee Network Security Platform I-series Sensors
- McAfee Network Security Platform M-series Sensors
- McAfee Network Security Manager Software
- McAfee Network Security Sensor Software

Protection Overview:

User Defined Signatures (UDS) are provided as an immediate solution to a security advisory. They are written and tested by McAfee with the objective of a quick turnaround. A UDS is intended to cover the known aspects of a threat and might not cover all variants. In some cases, UDS releases may generate incorrect identification.

How Can I Protect My Network?

For releases before May 31, 2013:

- Click the respective download link, and then click Save to save the zip file locally.
- Extract the UDS XML file to a temporary directory.
- Upload the UDS XML file to your Network Security Platform Sensor.

For releases after May 31, 2013:

- Click the link to the Knowledgebase article for the UDS you need to download.

  NOTE: UDS articles are registered articles and require you to log in to the ServicePortal.

- Download the zip file attached to the article, which contains installation instructions and the UDS.
- Extract the zip file and follow the installation instructions.
- Enable the UDS in blocking mode.

How Do I Know if My Network is Under Attack?

In the Threat Analyzer, look for the UDS.

Sourcefire

Partner Reference: SEU 1079 or SRU 2014-04-08-003

Published: 04/08/2014

Protection provided by: Sourcefire IPS

Protection Overview:

Rules to detect attacks targeting this vulnerability are included in this release and are identified with GID 1, SIDs 30510 through 30517.

Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are included in this release and are identified with GID 1, SIDs 24974 through 24975.

The Sourcefire VRT has also added and modified multiple rules in the blacklist, browser-firefox, browser-ie, exploit-kit, file-office and server-other rule sets to provide coverage for emerging threats from these technologies.

How Can I Protect My Network?

Ensure rules are downloaded and configured to drop or alert (policy can be configured to not drop when enforced if needed).

How Do I Know if My Network is Under Attack?

When these fire, alerts can be configured to email if necessary.