Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304

hp.com

Security Advisory

HP Networking Communication: OpenSSL Vulnerabilities (Heartbleed, etc.)

June 9, 2014

New OpenSSL Vulnerabilities

On June 5th, HP Networking support was notified of additional vulnerabilities discovered by security researchers in the open-source and widely-used OpenSSL toolkit:

- SSL/TLS MITM vulnerability (CVE-2014-0224)
- DTLS recursion flaw (CVE-2014-0221)
- DTLS invalid fragment vulnerability (CVE-2014-0195)
- SSL_MODE_RELEASE_BUFFERS NULL pointer dereference (CVE-2014-0198)
- SSL_MODE_RELEASE_BUFFERS session injection or denial of service (CVE-2010-5298)
- Anonymous ECDH denial of service (CVE-2014-3470)
- Obtaining ECDSA nonces via a FLUSH+RELOAD cache side-channel attack (CVE-2014-0076).

OpenSSL is used in some HP Networking products to provide encryption and SSL services. At this time we have completed investigation for various HP Network product families and determined the following are not vulnerable:

- ProVision-based switches
- MSM wireless controller and access points
- HP Threat Management Service zl module
- HP VAN SDN Controller

The following products are still under investigation:

- Comware-based switches and routers
- Unified wireless controller and access points

- Network Management Software (IMC, PCM)
- HP Networking VoIP solutions
- TippingPoint solutions (IPS, NGFW, SMS)

As HP Networking completes investigation, this page will be updated. We also highly recommend that customers follow steps in 'Recommended Best Practices' section to sign up for HP Networking security bulletins.

HP Networking takes its responsibility of maintaining current security policies very seriously and security remains a top priority for our customers and employees.

Previous Statement on Heartbleed Vulnerability

On April 8, 2014 HP Networking support was notified of the vulnerability known as Heartbleed in the open-source and widely-used OpenSSL toolkit. The vulnerability, if exploited, can allow unauthenticated access to portions of computer system memory. This vulnerability has garnered a substantial amount of media. See references section for link to National Vulnerability Database entry describing vulnerability in detail.

OpenSSL is used in some HP Networking products to provide encryption and SSL services. The same day the defect was discovered, HP Networking began a comprehensive review of all actively supported products.

We have completed investigations on all HP Networking hardware and software platforms and packages. We have **determined no HP Networking product exhibits Heartbleed defect** due to either using a version of OpenSSL that is not vulnerable or not using OpenSSL, including:

- All Data Center, Campus & Branch switches and routers
- All Unified and MSM wireless controllers and access points
- Network Management Software (IMC, PCM)
- All HP Networking VoIP solutions
- All TippingPoint solutions (IPS, NGFW, SMS)
- HP Threat Management Service zl module
- HP VAN SDN Controller*

*HP VAN SDN controller runs on an Ubuntu host operating environment and certain versions of Ubuntu (including version 12.04 LTS that is compatible with HP VAN SDN controller) have been identified as vulnerable. Please see references section for link to Ubuntu security notice describing patch steps.

Recommended Best Practices

We highly recommend that some basic best practices be followed:

1. Subscribe to HP's real-time security information: All HP products use a common centralized security bulletin process managed by HP's Software Security Response Team (SSRT). We highly encourage all customers to subscribe to SSRT security bulletins by following these steps:
    a. Go to HP.com
    b. Click 'support'
    c. Click 'support & troubleshooting'
    d. Click 'Sign up: driver, support & security alerts' near bottom of page
2. Follow hardening procedures outlined in following documents:
    a. Hardening ProCurve Switches
    b. Hardening Comware-based Devices

References

New OpenSSL vulnerabilities (June 2014)

- OpenSSL security advisory for new vulnerabilities
- National Vulnerability Database (CVE-2014-0224): SSL/TLS MITM vulnerability
- National Vulnerability Database (CVE-2014-0221): DTLS recursion flaw
- National Vulnerability Database (CVE-2014-0195): DTLS invalid fragment vulnerability
- National Vulnerability Database (CVE-2014-0198): SSL_MODE_RELEASE_BUFFERS NULL pointer dereference
- National Vulnerability Database (CVE-2010-5298): SSL_MODE_RELEASE_BUFFERS session injection or denial of service
- National Vulnerability Database (CVE-2014-3470):Anonymous ECDH denial of service
- National Vulnerability Database (CVE-2014-0076):Obtaining ECDSA nonces via a FLUSH+RELOAD cache side-channel attack

OpenSSL Heartbleed (April 2014)

- National Vulnerability Database (CVE-2014-0160): Heartbleed
- Ubuntu Security Notice USN-2165-1