National Cybersecurity and Communications Integration Center

10 April 2014

"Heartbleed" OpenSSL Vulnerability

Summary

Security researchers from Google Security recently discovered a vulnerability with the Heartbeat extension (RFC6520) to OpenSSL's Transport Layer Security (TLS) and the Datagram Transport Layer Security (DTLS) protocols.[1][2][3] According to open source reports, the vulnerability has existed within certain OpenSSL frameworks since at least 2012.[4] The Heartbeat extension is functionally a "keep-alive" between end-users and the secure server. It works by sending periodic "data pulses" of 64KB in size to the secure server and once the server receives that data; it reciprocates by re-sending the same data at the same size. The out-of-bounds "read" vulnerability exists because the Heartbeat extension in OpenSSL versions 1.0.1 through and 1.0.2-beta (including 1.0.1f and 1.0.2-beta1) do not properly validate the data being sent from the end-user. As a result, a malicious actor could send a specially-crafted heartbeat request to the vulnerable server and obtain sensitive information stored in memory on the server. Furthermore, even though each heartbeat only allows requests to have a data size limited to 64KB segments, it is possible to send repeated requests to retrieve more 64KB segments, which could include encryption keys used for certificates, passwords, usernames, and even sensitive content that were stored at the time. An attacker could harvest enough data from the 64KB segments to piece together larger groupings of information which could help an attacker develop a broader understanding of the information being acquired.[5]

> *OpenSSL is a large scale, collaborative effort to develop a commercially available toolkit that provides general purpose encryption using the SSL and TLS protocol.*[6]

According to a Trusted Third Party, exploit code written in Python Script has been observed in publicly available online outlets. There have also been a number of underground forums discussing the vulnerability, which indicates interest from nefarious actors.[7] Internal Trusted Third Party assessments reveal that the code is 100% effective against the specific versions of SSL protocol noted above. However, at this time it has not been observed having the capability to compromise all SSL protocols. It is also important to note that at this time there have been no reported malicious attacks that exploit this vulnerability.

The following vendors and products may include vulnerable OpenSSL versions within their product distributions:[8]

- CentOS Project – CentOS 6
- Debian Project – Debian GNU/Linux 7.0
- FreeBSD Project – FreeBSD 10.0 and prior
- Gentoo Foundation – Gentoo releases through 8 April 2014
- Novell, Inc – openSUSE 12.3 and 13.1

- Red Hat Inc – Fedora 19 and 20, Enterprise Linux/Desktop/HPC Node/Server/Workstation v.6; Enterprise Linux Server AUS v.6.5; Enterprise Linux Sever EUS v.6.5.z Enterprise Virtualization 3; and Storage Server 2.1
- Android mobile devices
- Third Party code using Python/Perl/Ruby
- OpenVPN
- Aruba Networks: ArubeOS 6.3.x and 6.4.x; ClearPass 6.1.x, 6.2.x, and 6.3.x
- Check Point Software Technologies: All versions of Security Gateway, Security Management, Multi-Domain Management/Provider-1, Data Center Security appliances, Endpoint Security Server, Endpoint Connect and SSL Network Extender, Gaia, Gaia Embedded, SecurePlatform 2.6, SecurePlatform Embedded, IPSO 4.x, IPSO 5.x, IPSO 6.2
- Cisco Systems: AnyConnect Secure Mobility Client for iOSl Desktop Collaboration Experience DX650, Unified 7900, 8900, 9900 series IP Phones, TelePresence Video Communication Server (VCS)
- Fortinet Inc: FortiGate (FortiOS) 5.0 and higher, FortiAuthenticator 3.0 and higher, FortiMail 5.0 and higher, FortiVoice, and FortiRecorder
- Juniper Networks: JUNOS OS 13.3R1, Odyssey Client 5.6r5 and later, IVEOS 7.4r1 and later as well as 8.0r1 and later, UAD 4.4ra and layer as well as 5.0r1 and later, JUNOS Pulse (Desktop) 4.0r5 and later as well as 5.0r1 and later, Network Connect 7.4r5 through 7.4r9.1 and 8.0r1 through 8.0r3.1, JUNOS Pulse (Mobile) for Android and iOS 4.2r1 and later
- F5 Networks: BIG-IP AAM 11.5.0 - 11.5.1; BIG-IP AFM 11.5.0 - 11.5.1; BIG-IP Analytics 11.5.0 - 11.5.1; BIG-IP APM 11.5.0 - 11.5.1; BIG-IP ASM 11.5.0 - 11.5.1; BIG-IP Edge Clients for Apple iOS 1.0.5, 2.0.0 - 2.0.1; BIG-IP Edge Clients for Linux 7080 - 7101; BIG-IP Edge Clients for MAC OS X 7080 - 7101; BIG-IP Edge Clients for Windows 7080 - 7101; BIG-IP GTM 11.5.0 - 11.5.1; BIG-IP Link Controller 11.5.0 - 11.5.1; BIG-IP LTM 11.5.0 - 11.5.1; BIG-IP PEM 11.5.0 - 11.5.1; BIG-IP PSM 11.5.0 - 11.5.1

Many of the vulnerable vendors noted above have already begun issuing patches and have information posted on their websites and portals addressing the vulnerability and a plan of action.

On a more positive note, the web browsers Firefox, Chrome, and Internet Explorer on Windows OS all use Windows cryptographic implementation, not OpenSSL.[9]

Mitigation Recommendations

The nature of this vulnerability is such that if encryption keys are captured by a malicious actor, then previously captured transmissions including usernames, passwords, and other sensitive content could be obtained and decrypted.[10] From an end-user's perspective, changing passwords before system patches have been implemented could still leave SSL transmissions vulnerable. Until patches are fully implemented, closely monitoring email accounts, bank accounts, social media accounts, and other assets are strongly recommended. End-users can set their web browsers so that they automatically detect revoked certificates; Firefox does this automatically.

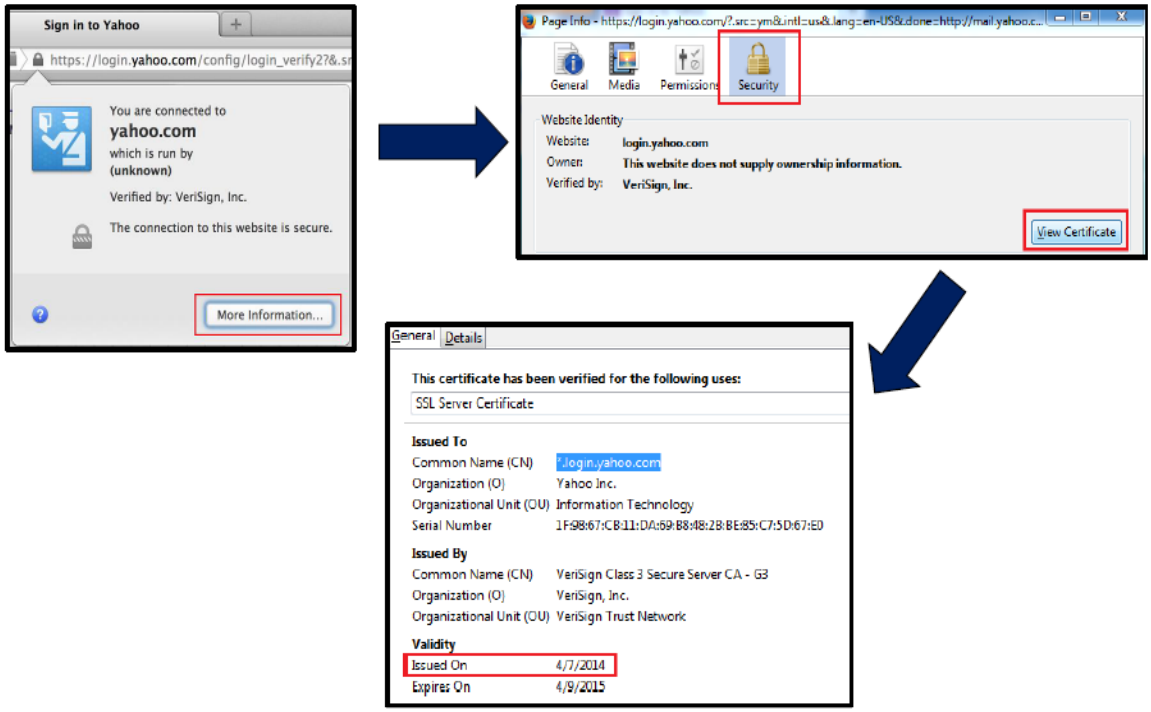

Figure 1: Step-by-step for verifying certificate. Though this is with Firefox, the process is similar on all web browsers.

From an enterprise perspective, it may be prudent to revoke previously used private keys and reissue new ones as soon as possible. Cached sessions (cookies, session keys) should also be considered compromised and probably cleared.[11]

It is important to understand that not all SSL-enabled webservers use OpenSSL with the Heartbeat extension[12], but as an added recommendation, it is probably a good idea to be observant of information passed on HTTPS servers until full patches are issued.

OpenSSL released a patch update, OpenSSL 1.0.1g, which addresses the issue in OpenSSL 1.0.1 (released in 2012). However, OpenSSL 1.0.2-beta has not yet been patched, but it is currently in the process of being corrected; the patch will be OpenSSL 1.0.2-beta2.[13]

Additional information on this vulnerability, including some indicators can be found at the following:

- hxxps://www.us-cert.gov/ncas/alerts/TA14-098A[14]
- hxxp://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160[15]
- hxxps://isc.sans.edu/[16]
- hxxp://www.securityfocus.com/bid/66690[17]
- hxxp://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160[18]
- hxxp://www.openssl.org/news/secadv_20140407.txt[19]

Points of Contact

For all inquiries pertaining to this product, please contact the NCCIC Duty Officer or NCCIC O&I Analysis at NCCIC@hq.dhs.gov or 1(888) 282-0870.

Can I share this product?

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

References

[1] https://www.openssl.org/news/secadv_20140407.txt
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
[3] iSight Partners
[4] SANS OpenSSL Vulnerability
[5] SANS OpenSSL Vulnerability
[6] https://www.openssl.org/about/
[7] iSight Partners
[8] iSight Partners
[9] SANS OpenSSL Vulnerability
[10] http://www.thewire.com/technology/2014/04/what-you-need-to-know-about-heartbleed-the-new-security-bug-scaring-the-internet/360366/
[11] iSight Partners
[12] http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html
[13] https://www.openssl.org/news/secadv_20140407.txt
[14] http://www.us-cert.gov/ncas/alerts/TA14-098A
[15] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
[16] https://isc.sans.edu/
[17] http://www.securityfocus.com/bid/66690
[18] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
[19] http://www.openssl.org/news/secadv_20140407.txt