National Cybersecurity and Communications

10 April 2014

"Heartbleed" OpenSSL Vulnerability

DISCLAIMER: *This advisory is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this advisory or otherwise. Further dissemination of this advisory is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.*

Summary

An OpenSSL vulnerability was recently discovered that can potentially impact internet communications and transmissions that were otherwise intended to be encrypted.[1][2][3] According to open source reports, the vulnerability has existed since 2012, but was only recently discovered.[4] Cyber-criminals could exploit this vulnerability to intercept and decrypt previously encrypted information.[5] At this time there have not been any reported attacks or malicious incidents involving this particular vulnerability, but because it is a highly visible media topic, it is possible that cyber-criminals could exploit it in the future.

Many vendors have already begun issuing patches and have information posted on their websites and portals addressing the vulnerability and a plan of action. For example, as of 9 April 2014 entities like Google, Facebook, and Yahoo implemented patches to fix the vulnerability.[6] Additionally, web browsers Firefox, Chrome, and Internet Explorer on Windows OS all use Windows cryptographic implementation, not OpenSSL; however, consumers should still use caution until the vulnerability has been fully addressed.[7]

Recommendations:

- Changing passwords is strongly recommended, but only after the vulnerability has been fully addressed.
  - *Changing passwords before the vulnerability is fixed could still leave consumers vulnerable.*
- Closely monitoring email accounts, bank accounts, social media accounts, and other online assets are strongly recommended.
- Once the vulnerability has been addressed, ensuring that visited websites requiring personal information such as login credentials or credit card information all are secure with the HTTPS identifier in the address bar.

For additional information and technical indicators, please visit the following:

- US-CERT - https://www.us-cert.gov/ncas/alerts/TA14-098A
- ICS-CERT - http://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-099-01

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: WHITE information without restriction, subject to copyright controls.

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] http://www.cio.com/article/751207/Vendors_and_Administrators_Scramble_to_Patch_OpenSSL_Vulnerability?taxonomyId=3089
[6] http://www.cnet.com/how-to/which-sites-have-patched-the-heartbleed-bug/
[7] SANS OpenSSL Vulnerability