HC3: Sector Alert

October 28, 2022 TLP: White Report: 202210280100

Critical OpenSSL Vulnerability Will Require Action by Healthcare Organizations

Executive Summary

A software library called OpenSSL – used with many of the most common operating systems and applications for secure communications – is going to receive an important update on Tuesday, November 1, 2022. OpenSSL is deployed across industries ubiquitously, including the health sector. HC3 highly recommends all public and private heatlh sector organizations identify all instances of OpenSSL in their infrastructure and prepare to test and deploy the patch as soon as it is released.

Report

OpenSSL is an open-source cryptographic library used with many of the most common operating systems and applications to implement Transport Layer Security and its predecessor protocol, Secure Sockets Layer for security in communicating with web and other Internet-facing servers. An announcement by the OpenSSL Project (can be found here) on October 25 noted that a new version of OpenSSL (version 3.0.7) would be released on Tuesday 1st November 2022 between 1300-1700 UTC. This update will contain a patch for a vulnerability classified as critical. It is very rare for the OpenSSL Project to classify a vulnerability as critical. As of the release of this alert, no further technical details exist on this vulnerability. The protection of technical details by the OpenSSL Project is likely deliberate to reduce attempts to identify and exploit this vulnerability prior to patch release on November 1.

Analysis

Due to the fact that this vulnerability is applicable across the public and private heatlh sectors and the apparent egregious nature of the vulnerability, exploitation, even on a very large scale, is very possible immediately after patch release on November 1. Threat actors, both state sponsored and cybercriminals, often reverse engineer a patch upon release to understand the technical details of the vulnerability and in order to develop an exploit. HC3 highly recommends that all health sector organizations treat this vulnerability with the highest priority.

Vulnerability

This vulnerability is limited to OpenSSL versions 3.0.0 through 3.0.6. HC3 is not aware of any other technical details or CVE assignment for this vulnerability as of the release of this alert. We are anticipating more details to be disclosed in the coming days, either by OpenSSL or other security researchers, especialy after the updated version (3.0.7) is released on November 1.

Patches, Mitigations, and Workarounds

As only versions 3.0.0 through 3.0.6 are known to be vulnerable at this time, the first step is for an organization to identify instances of OpenSSL and their version number. On many Linux variants, this can be done with the command:

```
# openssl version
```

Similarly, the following command can be used on a Windows command prompt:

```
openssl /?
```

HC3: Sector Alert

October 28, 2022 TLP: White Report: 202210280100

The OpenSSL project hosts a website where more information can be found and where the updated version with the patch will be available on November 1:

Homepage: https://www.openssl.org/

Vulnerabilities: https://www.openssl.org/news/vulnerabilities.html

Downloads: https://www.openssl.org/source/

References

Forthcoming OpenSSL Releases
https://mta.openssl.org/pipermail/openssl-announce/2022-October/000238.html

OpenSSL warns of critical security vulnerability with upcoming patch
https://www.zdnet.com/article/openssl-warns-of-critical-security-vulnerability-with-upcoming-patch/

Upcoming Critical OpenSSL Vulnerability: What will be Affected?
https://isc.sans.edu/forums/diary/Upcoming+Critical+OpenSSL+Vulnerability+What+will+be+Affected/29192/

Upcoming Critical OpenSSL Vulnerability: What will be Affected?
https://isc.sans.edu/forums/diary/Upcoming+Critical+OpenSSL+Vulnerability+What+will+be+Affected/29192/

OpenSSL is patching just its second critical security flaw ever
https://www.techradar.com/news/openssl-is-patching-just-its-second-critical-security-flaw-ever

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback