OpenSSL, a widely used encryption library, patches serious vulnerabilities

November 2 2022, by Amanda Pérez Pintado

Credit: Unsplash/CC0 Public Domain

Websites and companies that rely on OpenSSL should patch their systems as soon as possible.

The developer of Open SSL, a widely used open-source encryption library, released Tuesday a patch to fix two high severity security issues that could allow attackers to remotely execute new code or cause website crashes.

OpenSSL Project last week announced a security-fix update to fix an issue originally categorized as "critical." After further analysis, the severity was downgraded to "high" today with the release of the patch.

According to OpenSSL, an issue of critical severity if "remote code execution is considered likely in common situations," but the OpenSSL team said it no longer feels the rating applies to the issue.

"We are not aware of any working exploit that could lead to remote code execution, and we have no evidence of these issues being exploited as of the time of release of this post," OpenSSL said in a blog post.

The vulnerabilities only affect OpenSSL versions 3.0—released Sept. 2021—and above. Users are encouraged to upgrade to version 3.0.7.

"We still consider these issues to be serious vulnerabilities and affected users are encouraged to upgrade as soon as possible," OpenSSL said.

What issues did OpenSSL fix?

OpenSSL patched two security bugs. The flaw originally categorized as critical is an arbitrary 4-byte stacker overflow, which could allow hackers to remotely execute new code or cause website crashes.

"We are not aware of any working exploit that could lead to remote code execution, and we have no evidence of these issues being exploited as of the time of release of this post," OpenSSL said.

The second flaw could allow attackers to send emails with malicious certificates to crash websites.

What is OpenSSL used for?

OpenSSL is a widely used code library to provide secure communications across the internet and protect sensitive data such as emails, passwords or credit card data. Many internet servers rely on the software.

What does OpenSSL mean?

OpenSSL implements the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols used to encrypt sensitive data.

First released in 1998, the software changed its name before going public because the SSL acronym was more widely recognized than TLS.

What's the difference between SSL and TLS?

TLS is a network protocol that establishes an encrypted connection to protect private information sent over the internet, while SSL is an earlier and less secure version.

Web users may notice TSL/SSL encryption when they log in to their email or online bank account and see a small lock icon next to the "HTTPS." The lock icon signals that third parties won't be able to read information sent or received.

Is OpenSSL free?

"OpenSSL is licensed under an Apache-style license, which basically

means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions," according to OpenSSL.

What was the OpenSSL Heartbleed flaw?

Back in 2014, security researchers uncovered a major vulnerability in OpenSSL, dubbed Heartbleed. The flaw let anyone read the memory of servers running on OpenSSL and affected companies such as Yahoo, Google, Facebook and Tumblr.

Since then, the last critical vulnerability in OpenSSL was flagged in 2016.

(c)2022 USA Today
Distributed by Tribune Content Agency, LLC.

Citation: OpenSSL, a widely used encryption library, patches serious vulnerabilities (2022, November 2) retrieved 27 April 2024 from https://techxplore.com/news/2022-11-openssl-widely-encryption-library-patches.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.