An official website of the United States government Here's how you know

OpenSSL Releases Security Update

Original release date: November 01, 2022

OpenSSL has released a security advisory to address two vulnerabilities, CVE-2022-3602 and CVE-2022-3786, affecting OpenSSL versions 3.0.0 through 3.0.6.

Both CVE-2022-3602 and CVE-2022-3786 can cause a denial of service. According to OpenSSL, a cyber threat actor leveraging CVE-2022-3786, "can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution," allowing them to take control of an affected system.

CISA encourages users and administrators to review the OpenSSL advisory, blog, OpenSSL 3.0.7 announcement, and upgrade to OpenSSL 3.0.7. For additional information on affected products, see the 2022 OpenSSL vulnerability - CVE-2022-3602 GitHub repository, jointly maintained by the Netherland's National Cyber Security Centrum (NCSC-NL) and CISA.

This product is provided subject to this Notification and this Privacy & Use policy.