Neat Statement on the OpenSSL Critical Vulnerability

Last updated on November 1, 2022

CVE-2022-3602 (Remote Code Execution) and CVE-2022-3786 (Denial of Service)

The OpenSSL project team released a security fix for a critical vulnerability in OpenSSL and developers and organizations are being urged to ensure that they patch any instances of OpenSSL 3 in their software stack as a matter of urgency.

These two vulnerabilities affect OpenSSL versions 3.0.0 – 3.0.6 and are patched in the most recent release of version 3.0.7

What is OpenSSL?

OpenSSL is an open-source cryptography library widely used by applications, operating systems and websites to secure communications over the internet using SSL (Secure Sockets Layer) and TLS (Transport Layer Security).

What is the Impact of the OpenSSL Vulnerability?

The two new high-severity CVE's refer to areas of Distribution Denial of Service (DDoS) and Remote Code Execution(RCE). RCE attacks allow an attacker to remotely execute malicious code on a computer. The impact of an RCE vulnerability can range from malware execution to an attacker gaining full control over a compromised machine. DDoS is a category of malicious cyber-attacks that hackers or cybercriminals employ in order to make an online service, network resource or host machine unavailable to its intended users on the Internet.

Are Neat Products Impacted by the OpenSSL Vulnerability?

Firmware running on Neat Bar, Neat Bar Pro, Neat Board, Neat Frame, and Neat Pad are not impacted by the OpenSSL CVE-2022-3602 and CVE-2022-3786 vulnerabilities.

As this is an evolving incident, our team is continuing to investigate and validate additional information about this vulnerability and its impact, including assessing the risk to our business operations. If you have any further questions or security concerns, please send an email to *security@neat.no* or log a ticket with our customer support.

References / Credit

- Common Vulnerabilities & Exposures - CVE (https://www.cve.org/)
- OpenSSL (https://www.openssl.org/)
- CheckPoint Technologies (https://blog.checkpoint.com/)