Hive Pro

THREAT ADVISORY

OpenSSL exposed to Denial-of-service vulnerability causing Infinite Loop

TA2022062

Threat Level AMBER

Publish Date –March 17, 2022

A security flaw exists in OpenSSL software library that could lead to a denial-of-service (DoS) condition when parsing certificates.

The vulnerability, identified as CVE-2022-0778, arises from parsing a malformed certificate with invalid explicit elliptic-curve parameters, resulting in an "infinite loop". The flaw is in the function **BN_mod_sqrt()**, which is used to compute the modular square root. Because certificate parsing occurs prior to certificate signature verification, any process that parses an externally supplied certificate may be subject to a denial-of-service attack. As a result, vulnerable situations include:

- TLS clients consuming server certificates
- TLS servers consuming client certificates
- Hosting providers taking certificates or private keys from customers
- Certificate authorities parsing certification requests from subscribers
- Anything else which parses ASN.1 elliptic curve parameters

The vulnerability is fixed in versions 1.0.2zd (for premium support customers), 1.1.1n, and 3.0.2. While, OpenSSL 1.1.0 is also affected, no fix has been released as it has reached end-of-life.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
TA0001: Initial Access
T1190: Exploit Public-Facing Application
TA0040: Impact
T1499: Endpoint Denial of Service
T1499.004: Endpoint Denial of Service: Application or System Exploitation

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0778	OpenSSL versions 1.0.2, 1.1.1 and 3.0	cpe:2.3:a:openssl:openssl:1.0.2:*:*:*:*:*:*:*, cpe:2.3:a:openssl:openssl:1.1.1:*:*:*:*:*:*:*, cpe:2.3:a:openssl:openssl:3.0:*:*:*:*:*:*:*	Infinite loop in BN_mod_sqrt() reachable when parsing certificates	CWE-264

Patch Link

https://github.com/openssl/openssl/commit/a466912611aa6cbdf550cd10601390e587451246
https://github.com/openssl/openssl/commit/3118eb64934499d93db3230748a452351d1d9a65

References

https://www.openssl.org/news/secadv/20220315.txt