Security Advisory

Vulnerability List

OPENSSL INFINITE LOOP WHEN PARSING CERTIFICATES CVE-2022-0778

7.5

OVERVIEW

Advisory ID	SNWLID-2022-0002
First Published	2022-03-22
Last Updated	2022-10-14
Workaround	true
Status	Applicable
CVE	CVE-2022-0778
CWE	CWE-400
CVSS v3	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Direct Link	

SUMMARY

A vulnerability CVE-2022-0778 was found in OpenSSL that allows to trigger an infinite loop by crafting a certificate that has invalid elliptic curve parameters. Since certificate parsing happens before verification of the certificate signature, any process that parses an externally supplied certificate leads to a DoS (Denial of service) attack.

SonicWall is investigating its product line to determine which products and cloud services may be affected by this vulnerability.

AFFECTED PRODUCT(S)

Product	Affected Version(s)
SMA100	10.2.1.4-31sv and earlier versions
SMA1000	12.4.1, 12.1.0 and earlier versions
SonicOS Gen6	6.5.4.10-94 and earlier versions
SonicOS Gen7	7.0.1-5051 and earlier versions
GMS	prior 9.3.2
Analytics	prior 2.5.0.4
NSM	2.3.3-4-R18 and earlier versions
Capture Security Appliance	1.2.0-23 and earlier versions
Capture Client	3.7.3 and earlier versions
Email Security	10.0.16 and earlier versions
NetExtender Client	10.2.835 and earlier versions (Linux only)
Connect Tunnel Client	prior 12.41.01041
SonicWall Switch	Impacted
SonicWave Access Points	Impacted

Clients	Affected Version(s)
NetExtender for Linux	Linux clients prior to 10.2.839 are impacted
NetExtender for Windows	Not Impacted
Connect Tunnel v12.1 and earlier	Not Impacted
Connect Tunnel v12.4	Impacted
Mobile Connect for MacOS	MacOS clients prior to 5.0.10 are impacted
Mobile Connect for iOS	iOS clients prior to 5.0.11 are impacted

CPE(S)

WORKAROUND

Workarounds/Temporary Mitigations

SonicWall's (IPS) Intrusion Prevention System provides protection against this threat:

- IPS: 15407 OpenSSL BN_mod_sqrt Function DoS 1
- IPS: 15491 OpenSSL BN_mod_sqrt Function DoS 2
- IPS: 15351 OpenSSL BN_mod_sqrt Function DoS 3
- IPS: 15755 OpenSSL BN_mod_sqrt Function DoS 4

More information is available here:

https://securitynews.sonicwall.com/xmlpost/openssl-elliptic-curve-public-key-denial-of-service/

NOTE: Impacted customers will need to upgrade to fixed versions to remove residual risk.

FIXED SOFTWARE

SonicWall Product (Appliance/Cloud/Virtual/OnPrem)	Status	Fixed Version(s)
SMA1000 - SMA 6200/7200/6210/7210 - SMA 8200v (ESX, KVM, Hyper-V, AWS, Azure) - SRA EX 7000	Impacted	OpenSSL has been upgraded to 1.1.1n, remediating CVE-2022-0778, in the following releases: 12.4.1-02965, and 12.1.0-07081
SMA 100 - SMA 200/210/400/410 - SMA 500v (ESX, KVM, Hyper-V, AWS, Azure)	Impacted	OpenSSL has been upgraded to 1.1.1n, remediating CVE-2022-0778, in the following releases: 10.2.1.5-34sv, and 10.2.0.10-46sv.
Email Security - Hosted Email Security (HES) - On-Premise Email Security	Impacted	OpenSSL has been upgraded to 1.1.1n, remediating CVE-2022-0778, in 10.0.17
Gen5 Firewalls (EOS) - TZ100/W - TZ200/W - TZ210/W - NSA 220/W - NSA 250M/250M-W - NSA 2400/MX/3500/4500/5500	Impacted	OpenSSL has been upgraded to 1.1.1n, remediating CVE-2022-0778, in SonicOS 5.9.2.14 (SOHO) Only the listed Gen5 SOHO is currently supported. SonicWall is not releasing patches for other impacted EOL Gen 5 products listed. Please refer to SonicWall product life tables. And SOHO patch is expected to be released in late April.

~~NSA E5500/6500/6500/8500/8510~~ **Gen6 Firewalls**		OpenSSL has been upgraded to

COMMENTS

CREDIT(S)

REVISION HISTORY

Version

1.0

Date

22-Mar-2022

Description

Initial Release.

Version

1.1

Date

REFERENCE(S)

https://www.sonicwall.com/support/knowledge-base/security-notice-openssl-infinite-loop-when-parsing-certificates-cve-2022-0778/220412121029153/