SSL - CVE-2022-0778

PUBLISHED: APRIL 8, 2022 | LAST UPDATE: MAY 11 2022

SUMMARY

In March, 2022, OpenSSL.org released a security advisory [1] detailing an issue with the BN_mod_sqrt() function in OpenSSL used when parsing certificates. The following vulnerability can impart DoS impacts on ACOS ADC and SSLi data plane services, ACOS management plane services, aGalaxy local and ACOS device management services, and Harmony Controller local and ACOS device management services.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2022-0778	CVSS 3.0	7.5 High	openssl: Infinite loop in BN_mod_sqrt() reachable when parsing certificates [2]

AFFECTED RELEASES

The table below indicates releases of A10 products exposed to these vulnerabilities and their releases that address these issues or are otherwise unaffected by them.

Customers using affected A10 product releases can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no product release update is currently available.

Product Family	Releases Affected			Releases Resolved or Unaffected
ACOS	5.0.0	–	5.2.1-P4	5.2.1-P5
ACOS	5.0.1 TPS	–	5.0.2-P1 TPS	5.0.2-P2 TPS
ACOS	4.1.0	–	4.1.4-GR1-P9	4.1.4-GR1-P10
ACOS	4.1.100	–	4.1.100-P7	None
ACOS	3.1.0-P1	–	3.2.5-P6	5.0.2-P2 TPS
ACOS	2.8.2	–	2.8.2-P10	4.1.4-GR1-P10, 5.2.1-P5
ACOS	2.7.2	–	2.7.2-P17	4.1.4-GR1-P10, 5.2.1-P5
aGalaxy TPS	3.2.1	–	5.0.10	5.0.11

For all version of A10 Harmony Controller, customers should update the CentOS or RHEL operating system to correct this vulnerability on their systems hosting the Harmony Controller software product.

WORKAROUNDS AND MITIGATIONS

To mitigate this issue for the ACOS ADC and SSLi data plane services, use the "client-certificate Ignore" (which is the default) for all configured "slb template client-ssl" instances. For ACOS ADC, ensure the integrity of communications with, and the certificates on, TLS servers for configured "slb template server-ssl" instances. No mitigations are available for ACOS SSLi configured "slb template server-ssl" instances.

To mitigate this issue for the ACOS management plane, ensure the integrity of communication with, and the certificates on, TLS servers configured in ACOS or indicated during ACOS management operations. These include HTTPS file, LDAPS external authentication, and A10 ELM license management servers. Alternately, SCP or SFTP methods for secure file transfer can be used instead of HTTPS and Radius or TACACS+ can be used instead of LDAPS.

Further ACOS management plane mitigations can include ensuring the integrity of communication with A10 GLM license management and Brightcloud web-category services.

To mitigate this issue for aGalaxy and Harmony Controller, ensure the integrity of communications between these devices (instances) and the ACOS devices they manage was well as the A10 license management (ELM/GLM) services they may access.

Ensuring the integrity of these communications seeks to reduce the risk of man-in-the-middle attackers impersonating trusted servers and services exploiting this vulnerability.

SOFTWARE UPDATES

Software updates that address these vulnerabilities are or will be published at the following URL:

http://www.a10networks.com/support/axseries/software-downloads

VULNERABILITY DETAILS

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2022-0778	The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus 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 Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

RELATED LINKS

Ref #	General Link
[1]	OpenSSL Security Advisory [15 March 2022]
[2]	NIST NVD CVE-2022-0778

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2022-04-08	Initial Publication
2.0	2022-05-10	Expanded scope to include A10 aGalaxy and Harmony Controller (HC),products. Extended ACOS exposure scope discussion. Updated/refined workarounds/mitigations. Updated affected A10 product releases table.