TLS-SSL- CVE-2023-0286

PUBLISHED: APRIL 28, 2023 | LAST UPDATE: APRIL 28, 2023

Summary

On February 7, 2023, OpenSSL disclosed [1] OpenSSL vulnerabilities including CVE-2023-0286 involving a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. This vulnerability affects the ACOS SSL/TLS Data Plane and Management Plane and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2023-0286	CVSSv3	7.4 High	openssl: X.400 address type confusion in X.509 GeneralName [2]

Affected Releases

The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS 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 ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
5.0.0	–	5.2.1-P6	5.2.1-P7
4.1.4-GR1	–	4.1.4-GR1-P11	4.1.4-GR1-P12 for Data Plane
4.1.4-GR1	–	4.1.4-GR1-P12	4.1.4-GR1-P13 for Management Plane

Workarounds and Mitigations

None

Software Updates

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

https://support.a10networks.com/

Vulnerability Details

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

Vulnerability ID	Description
CVE-2023-0286	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.

Related Links

Ref #	General Link
[1]	https://www.openssl.org/news/secadv/20230207.txt
[2]	http://nvd.nist.gov/vuln/detail/CVE-2023-0286

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2023-4-28	Initial Publication