TLS-SSL- CVE-2023-0215

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

Summary

On November 1, 2022, OpenSSL disclosed [1] OpenSSL vulnerabilities including CVE-2023-0215. 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-2023-0215	CVSSv3	5.9 Medium	openssl: use-after-free following BIO_new_NDEF [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-2023-0215	The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected.

Related Links

Ref #	General Link
[1]	https://www.openssl.org/news/secadv/20230207.txt
[2]	http://nvd.nist.gov/vuln/detail/CVE-2023-0215

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2023-4-28	Initial Publication