OPENSSL – CVE-2021-23840

PUBLISHED: APRIL 30, 2021 | LAST UPDATE: APRIL 30, 2021

SUMMARY

In February 2021, a vulnerability in OpenSSL was disclosed [1] that CipherUpdate calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate with specially-crafted values could cause applications to behave incorrectly or crash. The following vulnerability may affect the management plane or TLS/SSL data plane of ACOS devices and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2021-23840	CVSS 3.0	7.5 High	openssl: integer overflow in CipherUpdate [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-P1	5.2.1-P2
5.0.1 TPS	–	5.0.1-P3 TPS	5.0.1-P4 TPS, 5.0.2 TPS
4.1.4-GR1	–	4.1.4-GR1-P7	4.1.4-GR1-P8
3.2.3-P1	–	3.2.5-P6	5.0.2 TPS

WORKAROUNDS AND MITIGATIONS

None

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-2021-23840	Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

RELATED LINKS

Ref #	General Link
[1]	OpenSSL Security Advisory [16 February 2021]
[2]	NIST NVD, CVE-2021-23840

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2021-04-30	Initial Publication

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.