OPENSSL – CVE-2021-3449

PUBLISHED: APRIL 23, 2021 | LAST UPDATE: APRIL 23, 2021

SUMMARY

In March 2021, a vulnerability in OpenSSL was disclosed [1] that could cause OpenSSL TLS server services to crash when sent a maliciously crafted renegotiation ClientHello message from a client, leading to a possible denial of service. It could also result in the disclosure of private memory contents. The following vulnerability may affect the data plane of ACOS devices and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2021-3449	CVSS 3.0	5.9 Medium	openssl: NULL pointer dereference in signature_algorithms processing [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
5.2.0	–	5.2.1-P1	5.2.1-P2
5.0.0	–	5.1.0-P5	5.1.0-P6

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-2021-3449	An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

RELATED LINKS

Ref #	General Link
[1]	OpenSSL Security Advisory [25 March 2021]
[2]	NIST NVD, CVE-2021-3449

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2021-04-23	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.