SSL - CVE-2019-1563

PUBLISHED: OCTOBER 18, 2019 | LAST UPDATE: FEBRUARY 14, 2020

SUMMARY

In September 2019, openssl.org released a security advisory [1] detailing several security issues. The following vulnerability may affect the TLS/SSL data plane of ACOS devices reported in that advisory and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2019-1563	CVSS 3.0	3.7 Low	openssl: Information disclosure in PKCS7_dataDecode and CMS_decrypt_set1_pkey [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	–	5.0.0-P1	5.1.0
4.1.4	–	4.1.4-GR1-P2	4.1.4-GR1-P3
4.1.2	–	4.1.2-P3	4.1.4-GR1-P3, 5.1.0
4.1.1	–	4.1.1-P12	4.1.1-P13
4.1.0	–	4.1.0-P12	4.1.1-P13, 4.1.4-GR1-P3, 5.1.0
2.8.2	–	2.8.2-P10	4.1.4-GR1-P3, 5.1.0
2.7.2	–	2.7.2-P14	4.1.1-P13, 4.1.4-GR1-P3, 5.1.0

WORKAROUNDS AND MITIGATIONS

Exclude RSA-based ciphers in the server-ssl configuration.

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-2019-1563	Some HTTP/2 implementations are vulnerable to unconstrained internal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

RELATED LINKS

Ref #	General Link
[1]	OpenSSL Security Advisory [10 September 2019]
[2]	NIST NVD, CVE-2019-1563

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2019-10-18	Initial Publication
2.0	2020-02-14	Update Releases Resolved versions