TCP/IP - CVE-2018-5390 (SEGMENTSMACK)

PUBLISHED: AUGUST 19, 2018 | LAST UPDATE: OCTOBER 11, 2019

SUMMARY

In August 2018, US CERT released a vulnerability note [1] regarding a security exposure in TCP processing of Linux kernels. The following vulnerabilities reported in that US CERT notice that affect the management plane of ACOS systems are addressed in this document.

TCP processing in the dataplane of ACOS systems is not exposed to this vulnerability.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2018-5390	CVSS 3.0	7.8 High	kernel: TCP segments with random offsets allow a remote denial of service (SegmentSmack) [2]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities 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
4.1.4	–	4.1.4-P1	4.1.4-P2
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P8	4.1.1-P9
4.1.100	–	4.1.100-P5	4.1.100-P5-SP1
4.1.0	–	4.1.0-P11	4.1.0-P12
3.2.2	–	3.2.2-P5	3.2.2-P6

WORKAROUNDS AND MITIGATIONS

Common security best practices in the industry for network appliance management and control planes can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical, infrastructure, networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

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-2018-5390	Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service.

RELATED LINKS

Ref #	General Link
[1]	US CERT, Vulnerability Note VU#962459
[2]	NIST NVD, CVE-2018-5390

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-08-19	Initial Publication
2.0	2019-10-11	Added 4.1.100 release family.