SYSTEM - CVE-2017-18017

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

SUMMARY

In January 2018, a vulnerability was published affecting the operating system in ACOS 3.x and 4.x. This vulnerability is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2017-18017	CVSS 3.0	9.8 Critical	kernel: netfilter: User-after-free in tcpmss_mangle_packet() in xt_TCPMSS.c

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
4.1.2	–	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-P4	3.2.2-P5

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-2017-18017	The tcpmss_mangle_packet function in net/netfilter/xt_TCPMSS.c in the Linux kernel before 4.11, and 4.9.x before 4.9.36, allows remote attackers to cause a denial of service (use-after-free and memory corruption) or possibly have unspecified other impact by leveraging the presence of xt_TCPMSS in an iptables action.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2017-18017

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.