RSYSLOG - CVE-2019-17041

PUBLISHED: MAY 8, 2020 | LAST UPDATE: MAY 8, 2020

SUMMARY

In September 2019, maintainers of rSyslog [1] disclosed a security vulnerability that could result in a heap overflow that might result in a crash, causing a Denial-of-Service attack. The following vulnerability may affect the management plane of ACOS devices and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2019-17041	CVSS 3.0	9.8 Critical	rsyslog: heap-based overflow in contrib/pmaixforwardedfrom/pmaixforwardedfrom. [2]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address these issues or are otherwise unaffected by them.

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	–	5.1.0-P4	5.1.0-P5
4.1.4	–	4.1.4-GR1-P4	4.1.4-GR1-P5, 5.1.0-P5
4.1.2	–	4.1.2-Px	4.1.4-GR1-P5, 5.1.0-P5
4.1.1	–	4.1.1-Px	4.1.4-GR1-P5, 5.1.0-P5
4.1.100	–	4.1.100-Px	None
4.1.0	–	4.1.0-Px	4.1.4-GR1-P5, 5.1.0-P5
3.1.0-P1	–	3.2.5-Px	5.0.1-TPS
2.8.2	–	2.8.2-Px	4.1.4-GR1-P5, 5.1.0-P5
2.7.2	–	2.7.2-Px	4.1.4-GR1-P5, 5.1.0-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-2019-17041	An issue was discovered in Rsyslog v8.1908.0. contrib/pmaixforwardedfrom/pmaixforwardedfrom.c has a heap overflow in the parser for AIX log messages. The parser tries to locate a log message delimiter (in this case, a space or a colon) but fails to account for strings that do not satisfy this constraint. If the string does not match, then the variable lenMsg will reach the value zero and will skip the sanity check that detects invalid log messages. The message will then be considered valid, and the parser will eat up the nonexistent colon delimiter. In doing so, it will decrement lenMsg, a signed integer, whose value was zero and now becomes minus one. The following step in the parser is to shift left the contents of the message. To do this, it will call memmove with the right pointers to the target and destination strings, but the lenMsg will now be interpreted as a huge value, causing a heap overflow.

RELATED LINKS

Ref #	General Link
[1]	pmaixforwardedfrom bugfix: potential misadressing #3884
[2]	NIST NVD CVE-2019-17041

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2020-05-08	Initial Publication