NTP - CVE-2020-13817

PUBLISHED: JULY 27, 2020 | LAST UPDATE: AUGUST 16, 2021

SUMMARY

In March 2020, NTP.org[1] released a security advisory detailing a number of security issues. The following vulnerability reported in the NTP advisory is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2020-13817	CVSS 3.0	7.4 High	ntp: ntpd using highly predictable transmit timestamps could result in time change or DoS [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
5.2.0			5.2.0-P1
5.0.0	–	5.1.0-P4	5.1.0-P5
4.1.4	–	4.1.4-GR1-P4	4.1.4-GR1-P5
4.1.2	–	4.1.2-P1	4.1.4-GR1-P5
4.1.1	–	4.1.1-P13	4.1.4-GR1-P5
4.1.100	–	4.1.100-P7	None
4.1.0	–	4.1.0-P13	4.1.4-GR1-P5
3.1.0-P1	–	3.2.5-P1	3.2.5-P2, 5.0.1-TPS
2.8.2	–	2.8.2-P10	4.1.4-GR1-P5
2.7.2	–	2.7.2-P16	4.1.4-GR1-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-2020-13817	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance.

RELATED LINKS

Ref #	General Link
[1]	4.2.8p14 Release Announcement
[2]	NIST NVD CVE-2020-13817

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2020-07-27	Initial Publication
2.0	2021-08-16	Add resolved releases for 3.2.5