NTP - CVE-2017-6462, CVE-2017-6451, CVE-2016-9042

PUBLISHED: AUGUST 10, 2017 | LAST UPDATE: JANUARY 25, 2021

SUMMARY

In March, 2017, NTP.org[1] released a security advisory detailing a number of security issues. The following vulnerabilities reported in the NTP advisory are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2017-6462	CVSS 3.0	7.8 High	ntp: Buffer Overflow in DPTS Clock [2]
2	CVE-2017-6451	CVSS 3.0	7.8 High	ntp: Improper use of snprintf() in mx4200_send()[3]
3	CVE-2016-9042	CVSS 3.0	4.4 Med	ntp: DoS via origin timestamp check functionality [4, 5]

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	4.1.2-P2
4.1.1	–	4.1.1-P3	4.1.1-P4
4.1.100	–	4.1.100-P5	4.1.100-P5-SP1
4.1.0	–	4.1.0-P9	4.1.0-P10
3.2.3	–	3.2.5-P1	3.2.5-P2, 5.0.1-TPS
3.1.0-P1	–	3.2.1-P1	3.2.2-P1, 5.0.1-TPS
2.8.2	–	2.8.2-P8	4.1.2-P2, 4.1.4-GR1-P5, 5.1.0-P5, 5.2.0-P1
2.7.2	–	2.7.2-P11	4.1.0-P10, 4.1.1-P4, 4.1.4-GR1-P5, 5.1.0-P5, 5.2.0-P1
2.7.1-GR1	–	2.7.1-GR1-P1	4.1.0-P10, 4.1.1-P4, 4.1.4-GR1-P5, 5.1.0-P5, 5.2.0-P1
2.6.1-GR1	–	2.6.1-GR1-P16	4.1.0-P10, 4.1.1-P4, 4.1.4-GR1-P5, 5.1.0-P5, 5.2.0-P1

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-2017-6462	Buffer overflow in the legacy Datum Programmable Time Server (DPTS) refclock driver in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via a crafted /dev/datum device.
CVE-2017-6451	The mx4200_send function in the legacy MX4200 refclock in NTP before 4.2.8p10 and 4.3.x before 4.3.94 does not properly handle the return value of the snprintf function, which allows local users to execute arbitrary code via unspecified vectors, which trigger an out-of-bounds memory write.
CVE-2016-9042	An exploitable denial of service vulnerability exists in the origin timestamp check functionality of ntpd 4.2.8p9. A specially crafted unauthenticated network packet can be used to reset the expected origin timestamp for target peers. Legitimate replies from targeted peers will fail the origin timestamp check (TEST2) causing the reply to be dropped and creating a denial of service condition. This vulnerability can only be exploited if the attacker can spoof all of the servers.

RELATED LINKS

Ref #	General Link
[1]	March 2017 ntp-4.2.8p10 NTP Security Vulnerability Announcement
[2]	NIST NVD, CVE-2017-6462
[3]	NIST NVD, CVE-2017-6451
[4]	Red Hat, CVE-2016-9042
[5]	Red Hat: Bug 1434017 - (CVE-2016-9042) CVE-2016-9042 ntp: DoS via origin timestamp check functionality

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-10	Initial Publication
2.0	2019-10-11	Added 4.1.100 release family
3.0	2020-07-27	Added 4.1.4, 5.x release families, update resolved versions
4.0	2021-01-22	Added 3.2.3-5, 5.0.1-TPS release families, update resolved versions