NTP - CVE-2016-7429, CVE-2016-7433

PUBLISHED: JULY 27, 2017 | LAST UPDATE: JULY 27, 2017

SUMMARY

In November, 2016, NTP.org 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-2016-7429	CVSS 3.0	3.7 Low	ntpd Rx server response from spoof on wrong I/F [1, 2]
2	CVE-2016-7433	CVSS 3.0	5.3 Medium	ntpd bug - jitter value higher than expected [1, 3]

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
			4.1.2 [(a)]
4.1.1	–	4.1.1-P1	4.1.1-P2
4.1.0	–	4.1.0-P9	4.1.0-P10
3.1.0-P1	–	3.2.1-P1	3.2.2-P1
2.8.2	–	2.8.2-P8	4.1.2
2.7.2	–	2.7.2-P11	4.1.0-P10, 4.1.1-P2
2.7.1-GR1	–	2.7.1-GR1-P1	4.1.0-P10, 4.1.1-P2
2.6.1-GR1	–	2.6.1-GR1-P16	4.1.0-P10, 4.1.1-P2

[(a)] Including all updates to the release(s).

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-2016-7429	NTP before 4.2.8p9 changes the peer structure to the interface it receives the response from a source, which allows remote attackers to cause a denial of service (prevent communication with a source) by sending a response for a source to an interface the source does not use.

CVE-2016-7433	NTP before 4.2.8p9 does not properly perform the initial sync calculations, which allows remote attackers to unspecified impact via unknown vectors, related to a "root distance that did not include the peer dispersion."

RELATED LINKS

Ref #	General Link
[1]	November 2016 ntp-4.2.8p9 NTP Security Vulnerability Announcement
[2]	NIST NVD, CVE-2016-7429
[3]	NIST NVD, CVE-2016-7433

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-07-27	Initial Publication