NTP - CVE-2020-11868

PUBLISHED: JULY 20, 2020 | LAST UPDATE: AUGUST 16, 2020

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-2020-11868	CVSS 3.0	7.5 High	ntp: DoS on client ntpd using server mode packet [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

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.

Ensure that the following are included for NTP configuration for ACOS devices:

- Use authentication with symmetric keys. This approach applies a symmetric key for the calculation of the MAC, which protects authenticity and integrity of the exchanged packets for an association. It is recommended that each association be protected by its own unique key.

- Maximize the number of time sources configured and their availability. ACOS supports a maximum of 4 NTP servers, which will provide sufficient backup in the event that one source goes down.

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-2020-11868	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp.

RELATED LINKS

Ref #	General Link
[1]	March 2020 ntp-4.2.8p14 NTP Release and Security Vulnerability Announcement
[2]	NIST NVD CVE-2020-11868

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

© Copyright 2021 A10 Networks, Inc. All Rights Reserved.

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.