Security Advisory

NTP - CVE-2018-7184

PUBLISHED: SEPTEMBER 12, 2018 | LAST UPDATE: OCTOBER 11, 2019

SUMMARY

A number of vulnerabilities have surfaced in the Operating System (OS) supported in ACOS 3.x and 4.x. Accordingly, the following vulnerabilities are addressed in this document.

Item		Score		
#	**Vulnerability ID**	**Source**	**Score**	**Summary**
1	CVE-2018-7184	CVSS 3.0	7.5 High	NTP: Interleaved symmetric mode cannot recover from bad state [1]

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
4.1.4	–	4.1.4-P1	4.1.4-P2
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P8	4.1.1-P9
4.1.100	–	4.1.100-P5	4.1.100-P5-SP1
4.1.0	–	4.1.0-P11	4.1.0-P12
3.1.0-P1	–	3.2.2-P5	3.2.2-P6, 3.2.3
2.8.2	–	2.8.2-Px	4.1.2-P5, 4.1.4-P2
2.7.2	–	2.7.2-Px	4.1.0-P12, 4.1.4-P9, 4.1.2-P5, 4.1.4-P2
2.7.1-GR1	–	2.7.1-GR1-Px	4.1.0-P12, 4.1.4-P9, 4.1.2-P5, 4.1.4-P2

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-2018-7184	ntpd in ntp 4.2.8p4 before 4.2.8p11 drops bad packets before updating the "received" timestamp, which allows remote attackers to cause a denial of service (disruption) by sending a packet with a zero-origin timestamp causing the association to reset and setting the contents of the packet as the most recent timestamp. This issue is a result of an incomplete fix for CVE-2015-7704.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2018-7184

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-09-12	Initial Publication
2.0	2019-10-11	Added 4.1.100 release family.

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.