HTTPD - CVE-2017-3169, CVE-2017-7679

PUBLISHED: JULY 16, 2018 | LAST UPDATE: OCTOBER 11, 2019

SUMMARY

In June 2017, Apache HTTPD released a security advisory detailing several security issues. The following vulnerabilities reported in the Apache HTTP advisory affect the ACOS HTTP and HTTPS management services and are addressed in this document.

Item		Score		
#	Vulnerability ID	Source	Score	Summary
1	CVE-2017-3169	CVSS 3.0	9.8 Critical	httpd: mod_ssl NULL pointer dereference [1]
2	CVE-2017-7679	CVSS 3.0	9.8 Critical	httpd: mod_mime buffer overread [2]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

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	–	4.1.2-P2	4.1.2-P3
4.1.1	–	4.1.1-P5	4.1.1-P6
4.1.100	–	4.1.100-P5	4.1.100-P5-SP1
4.1.0	–	4.1.0-P9	4.1.0-P10
3.1.0-P1	–	3.2.2-P2	3.2.2-P3

[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-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2017-3169
[2]	NIST NVD, CVE-2017-7679

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-16	Initial Publication
2.0	2018-07-18	Corrected ACOS 3.x affected release.
3.0	2018-11-02	Added indication of ACOS functions affected.
4.0	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.