HTTPD- CVE-2022-28614, CVE-2021-34798

PUBLISHED: JULY 26, 2022 | LAST UPDATE: JULY 26, 2022

Summary

In September 2021 and June 2022, OpenSSL disclosed [1] HTTPD vulnerabilities that may cause an integer overflow and subsequent out-of-bounds read or a potential Denial-of Service (DoS) crash of the HTTPD. These vulnerabilities may affect the GUI and AXAPI management plane services of ACOS devices and are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2022-28614	CVSSv3	9.1 Critical	httpd: Out-of-bounds read via ap_rwrite() [2]
1	CVE-2021-34798	CVSSv3	7.5 High	httpd: NULL pointer dereference via malformed requests [3]

Affected Releases

The table below indicates releases of ACOS exposed to this vulnerability 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
5.0.0	–	5.2.1-P5	5.2.1-P6
5.0.1 TPS	–	5.0.2-P1 TPS	5.0.2-P2-TPS
4.1.4-GR1	–	4.1.4-GR1-P10	4.1.4-GR1-P11
3.2.3-P1	–	3.2.5-P6	5.0.2-P2 TPS

Workarounds and Mitigations

None

Software Updates

Software updates that address these vulnerabilities are or will be published at the following URL:

https://support.a10networks.com/

Vulnerability Details

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2022-28614	The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
CVE-2021-34798	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

Related Links

Ref #	General Link
[1]	Apache.org - Apache HTTP Server 2.4 vulnerabilities
[2]	NIST NVD, CVE-2022-28614
[2]	NIST NVD, CVE-2021-34798

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2022-07-26	Initial Publication