HTTPD- CVE-2022-22720

PUBLISHED: MAY 12, 2022 | LAST UPDATE: JULY 26, 2022

Summary

In March 2022, apache.org disclosed [1] an HTTPD vulnerability that may expose the server to HTTP request smuggling when the HTTP daemon does not close an inbound connection following errors encountered when attempting to discard an HTTP request body. This vulnerability may affect the GUI and AXAPI management plane services of ACOS devices and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2022-22720	CVSSv3	9.8 Critical	httpd: Errors encountered during the discarding of request body lead to HTTP request smuggling [2]

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-2022-22720	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling.

Related Links

Ref #	General Link
[1]	Apache.org - Apache HTTP Server 2.4 vulnerabilities
[2]	NIST NVD, CVE-2022-22720

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2022-05-12	Initial Publication
1.1	2022-07-26	Updated 5.2.1 resolved release to 5.2.1-P6