CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-078

Apache HTTP Server Critical Vulnerability

December 23, 2021 — v1.0

TLP:WHITE

History:

- *23/12/2021 — v1.0 – Initial publication*

Summary

On Monday 20 December 2021, The Apache Software Foundation has released Apache HTTP Server 2.4.52 [1]. This version fixes two vulnerabilities:

- CVE-2021-44790: critical severity, CVSS base score of 9.8 [2].
- CVE-2021-44224: high severity, CVSS base score of 8.2 [3].

While the vulnerabilities affect optional modules, the risk is substantial if these modules are used in specific configurations, as the attack does not require authentication and could potentially lead to remote code execution [4]. At the time of this writing, no publicly available exploits are known to exist and the vulnerabilities are not under active attack yet.

Technical Details

CVE-2021-44790 (Critical - CVSS base score = 9.8) [2]

A carefully crafted request body can cause a buffer overflow in the `mod_lua` multipart parser (`r:parsebody()` called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one [2].

CVE-2021-44224 (High - CVSS base score = 8.2) [3]

A crafted URI sent to the HTTP Server, when configured as a forward proxy (`ProxyRequests on`), can cause a crash (`NULL` pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Affected Products

- CVE-2021-44790 affects Apache HTTP Server 2.4.51 and earlier.
- CVE-2021-44224 affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

Recommendations

CERT-EU strongly recommends updating Apache HTTP Server installations to version 2.4.52 or later.

References

[1] https://httpd.apache.org/security/vulnerabilities_24.html

[2] https://nvd.nist.gov/vuln/detail/CVE-2021-44790

[3] https://nvd.nist.gov/vuln/detail/CVE-2021-44224

[4] https://threatpost.com/apache-httpd-server-bugs-rce-dos/177234/