CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-054

Vulnerabilities in Apache HTTP Server

October 8, 2021 — v1.2

TLP:WHITE

History:

- *06/10/2021 — v1.0 – Initial publication*
- *07/10/2021 — v1.1 – Update* `mod-cgi`
- *08/10/2021 — v1.2 – Update incomplete fix*

Summary

On October 4, Apache released updates to address a couple of security vulnerabilities [1]. One of the vulnerabilities, the `CVE-2021-41773`, is actively exploited in the wild. This vulnerability allows a remote attacker to perform directory traversal attacks [2]. Additionally, this flaw could be leveraged by attackers to execute arbitrary code [3,4].

On October 8, Apache released version 2.4.51 after discovering that the previous fix for the `CVE-2021-41773` was incomplete [5]. This new flaw is tracked as `CVE-2021-42013`.

Technical details

The vulnerabilities exist due to input validation error when processing directory traversal sequences. A remote attacker can send a specially crafted HTTP request to map URLs to files outside the expected document root. If files outside of the document root are not protected by the `require all denied` option, these requests can succeed. Additionally, these flaws could leak the source of interpreted files like CGI scripts.

The flaws can also be used to execute arbitrary code [3,4] when:

- `mod-cgi` is enabled,
- `require all denied` option is not set for directories outside of the document root.

While it is not proven that other modules, like `mod-php`, might be used to execute arbitrary code, they should be considered at risk [3].

Products affected

`CVE-2021-41773`

Apache HTTP Server: 2.4.49 (and not earlier versions).

`CVE-2021-42013`

Apache HTTP Server: 2.4.49 and 2.4.50 (and not earlier versions).

Recommendations

Apache has released software updates to version 2.4.51 addressing the vulnerabilities [1,5]. There is no workaround recommended by the vendor to address them.

Using a Web Application Firewall (WAF) might mitigate the risk.

CERT-EU recommends updating vulnerable applications as soon as possible.

References

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

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773

[3] https://twitter.com/wdormann/status/1445573881121546245

[4] https://twitter.com/justinsteven/status/1445544161206169605

[5] https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-42013