CERT-EU

Security Advisory 2024-073

Apache HTTP Server Critical Vulnerabilities

July 24, 2024 — v1.0

TLP:CLEAR

History:

- *24/07/2024 — v1.0 – Initial publication*

Summary

On July 23, 2024, Apache issued an advisory about two critical vulnerabilities in its HTTP Server, **CVE-2024-40725** and **CVE-2024-40898**. These vulnerabilities can lead to HTTP request smuggling and SSL client authentication bypass, potentially resulting in unauthorised access and other malicious activities [1].

It is recommended to update affected systems immediately.

Technical Details

- **CVE-2024-40725**: A partial fix regression for a previous issue (CVE-2024–39884), which allows source code disclosure via certain legacy content-type-based configuration settings.
- **CVE-2024-40898**: An SSRF vulnerability in the `mod_rewrite` module on Windows systems, enabling attackers to extract NTLM hashes through carefully crafted requests.

Exploitation of these vulnerabilities could allow attackers to gain unauthorised access, perform session hijacking, cross-site scripting (XSS), or command injection. More information about the attack method can be found here [2].

Affected Products

- Apache HTTP Server versions 2.4.0 to 2.4.61.

Recommendations

An open-source vulnerability checker is available on github [3].

CERT-EU recommends updating affected devices to the latest version of Apache HTTP Server (2.4.62 or later) as soon as possible.

References

[1] https://censys.com/cve-2024-40725-40898/

[2] https://medium.com/@elniak/cve-2024-40725-and-cve-2024-40898-critical-vulnerabilities-in-apache-http-server-d292084255dc

[3] https://github.com/TAM-K592/CVE-2024-40725-CVE-2024-40898