CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-019

Apache Web Server Vulnerability

April 6, 2020 — v1.0

TLP:WHITE

History:

- *06/04/2020 — v1.0 – Initial publication*

Summary

On the 1st of April 2020, a new vulnerability was made public related to Apache Web server. Apache HTTP Server is prone to an open-redirection vulnerability because it fails to properly validate the redirect URLs. Specifically, this issue affects the `mod_rewrite` configurations. An attacker can leverage this issue by constructing a crafted URI and target a user to follow it.

Technical Details

Apache HTTP Server is prone to an open-redirection vulnerability because it fails to properly validate the redirect URLs. *Redirects* configured with `mod_rewrite` that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL [1].

When an unsuspecting victim follows the link, he or she may be redirected to an attacker-controlled site. The attack could have serious impact and the probability that this vulnerability to be exploit is very high [2].

The vulnerability received the number CVE-2020-1927. Note: This is the same defect as CVE-2019-10098. The fix for CVE-2019-10098 was ineffective [2].

Products Affected

It affects Apache HTTP servers versions from 2.4.0 to 2.4.41.

Recommendations

Apache Server Project has released a patch for this vulnerability [3]. It was fixed in Apache HTTP Server 2.4.42. It is strongly advised to update to the version 2.4.42 to patch this vulnerability as soon as possible.

Workarounds

In case an immediate update is not possible there is a possible mitigation [2]:

- anchor captures used as back-references,
- prefix self-referential redirects with `/` or scheme, host, and port.

References

[1] https://nvd.nist.gov/vuln/detail/CVE-2019-10098#vulnCurrentDescriptionTitle

[2] https://seclists.org/oss-sec/2020/q2/3

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