APACHE HTTPD VULNERABILITY

CVE-2021-44790
Severity 9.8/10 – Critical
CVE-2021-44224
Severity 8.2/10 – High

Executive Summary

On 20th December 2021, Apache published information about 2 new vulnerabilities CVE-2021-44790 a remote code execution (RCE) vulnerability in Apache HTTPD & CVE-2021-44224, Possible NULL dereference or SSRF in forward proxy configurations in Apache HTTP Server. These vulnerabilities may allow an attacker to remotely control an affected system.

While details around these threats are still emerging and affected products, applications are still being understood, it is recommended to patch Apache to version 2.4.52 as this mitigates both vulnerabilities. There are currently no known exploits of this in the wild.

CVE Number	Version Affected
CVE-2021-44790	**< = 2.4.51**
CVE-2021-44224	**> = 2.4.7, < = 2.4.51**

Details

CVE-2021-44790

Exploitation of CVE-2021-44790 could give remote attackers full control of vulnerable systems. To achieve RCE it appears that the “mod_lua Multipart Parser” would need to be loaded. While this module is not necessarily utilised in many applications, the main concerns here lie with the fact that attack complexity is low, no user interaction is required. As always RCE vulnerabilities carry considerable concern since these covers most of the stages of a breach in one go.

CVE-2021-44224

An edited URI (Uniform Resource Identifier) sent to an Apache server set up as a forward proxy can cause a crash resulting in a DoS (Denial of Service) which would likely affect access to anything “behind” the forward proxy. If the “configurations mixing forward and reverse proxy declarations” then there is a risk of SSRF (a request passed on and authenticated as if it came from the legitimate server).

Mitigation and Remediation

The below is recommended to implement to mitigate potential compromise.

- Apply the latest Apache Security updates (2.4.52) for HTTPD.
- Disable mod_lua wherever possible as recommended by Apache, if not utilised as part of BAU activity
- Get a list of all loaded/enabled modules in HTTPD on RHEL, CentOS etc.:
  - $ httpd -M
  - $ apachectl -M

As always remember to update packages when deploying Linux Servers

References

- https://msrc.Apache.com/update-guide/en-US/vulnerability/CVE-2021-44790
- https://attackerkb.com/topics/wQYx7xG5I3/CVE-2021-44790/vuln-details
- https://nvd.nist.gov/vuln/detail/CVE-2021-44790#vulnConfigurationsArea
- https://techcommunity.Apache.com/t5/exchange-team-blog/released-october-2021-exchange-server-security-updates/ba-p/2838287
- https://twitter.com/arudd1ck