BOLETÍN DE ALERTA

Boletín Nro.: 2021-41

Fecha de publicación: 23/12/2021

Tema: Actualización de seguridad para Apache HTTP Server

Software afectado:

- Apache HTTP Server versiones anteriores a 2.4.52

Descripción:

Apache ha publicado una actualización de seguridad para mitigar dos vulnerabilidades, una de severidad alta y la otra de severidad critica, identificadas como CVE-2021-44224 y CVE-2021-44790 respectivamente.

A continuación, se describen las vulnerabilidades:

- CVE-2021-44224 de severidad alta, con una puntuación de 8.2. La falla reside en el componente del *Proxy Handler*. Un atacante podría crear una petición *httpd* maliciosa provocando un ataque de denegación de servicio (DoS).

- CVE-2021-44790 de severidad critica, con una puntuación 9.8. La falla reside en el componente *mod_lua Multipart Parser* a través de un error de programación en la función *r:parsebody.* Un atacante no autenticado podría llevar a cabo un ataque de desbordamiento de búfer con el fin de realizar ejecución remota de comandos.

Impacto:

La explotación de estas vulnerabilidades en conjunto permitiría a un atacante obtener el control total del sistema afectado.

Solución:

Se recomienda actualizar el Apache HTTP Server a la versión 2.4.52:

- Unix/Linux: https://httpd.apache.org/docs/current/en/install.html

- Windows: https://httpd.apache.org/docs/current/es/platform/windows.html

Información adicional:

- https://www.cisa.gov/uscert/ncas/current-activity/2021/12/22/apache-releases-security-update-http-server
- https://httpd.apache.org/security/vulnerabilities_24.html
- https://vuldb.com/es/?id.188755
- https://vuldb.com/es/?id.188754
- https://nvd.nist.gov/vuln/detail/CVE-2021-44224
- https://nvd.nist.gov/vuln/detail/CVE-2021-44790