BOLETÍN DE ALERTA

Boletín Nro.: 2021-29

Fecha de publicación: 05/10/2021

Tema: Vulnerabilidades críticas en Apache Server.

Fecha de actualización: 08/10/2021

Versión afectada:

- Apache HTTP Server 2.4.49
- Apache HTTP Server 2.4.50

Descripción:

Apache Software Foundation ha lanzado actualizaciones del servidor web HTTP para abordar tres vulnerabilidades: CVE-2021-41773, CVE-2021-41524 y CVE-2021-42013 esta última se debe a una corrección insuficiente de la CVE-2021-41773 lanzada en la versión 2.4.50 de Apache Server.

La vulnerabilidad de día cero explotada activamente identificada como CVE-2021-41773, permite a los actores malintencionados acceder a archivos fuera del directorio raíz, manipulando la URL.

Los ataques directorio transversal implican el envío de solicitudes para acceder a directorios de servidores sensibles o de back-end que deberían estar fuera de su alcance. Normalmente, estas solicitudes se bloquean, pero en este caso, los filtros se omiten mediante el uso de caracteres codificados (ASCII) para las URL. Además, las vulnerabilidades de esta falla pueden dar lugar a la filtración de la fuente de los archivos interpretados, como los scripts CGI. Igualmente podría derivar en la filtración de archivos de configuración u otros que puedan contener información sensible.

Para que el ataque funcione, el objetivo debe ejecutar Apache HTTP Server 2.4.49, y también debe tener deshabilitado el parámetro de control de acceso "requerir todo denegado". Se debe tener en cuenta que esta es la configuración predeterminada .

Las versiones anteriores de Apache Server o las que tienen una configuración de acceso diferente no son vulnerables a esta falla.

La segunda vulnerabilidad identificada como CVE-2021-41524, se debe a que no se detectó ningún puntero de referencia durante el procesamiento de solicitudes HTTP/2. Esta falla permite que un atacante realice un ataque de denegación de servicio (DoS) en el servidor comprometido.

Esta falla también existe solo en la versión 2.4.49 del servidor Apache, pero no se tiene conocimiento de explotación activa.

La actualización 2.4.50 lanzada días atrás por Apache Foundation para corregir la vulnerabilidad de ataque directorio transversal (**path traversal attack**) CVE-2021-41773, sin embargo, el parche está incompleto y provocó la nueva vulnerabilidad identificada como CVE-2021-42013. Como resultado de esta falla, los atacantes pueden volver a ejecutar un ataque directorio transversal, lo que afecta a los usuarios del servidor web Apache 2.4.49 y 2.4.50. Para solucionar la falla Apache ha lanzado la versión 2.4.51 de su Servidor Web.

Debido a la explotación activa, se recomienda encarecidamente a los usuarios que actualicen a la última versión (2.4.51) para mitigar el riesgo asociado con la falla.

Impacto:

La explotación exitosa de estas vulnerabilidades podrían permitir a un atacante acceder a archivos fuera de la raíz del documento o interrumpir el servicio .

Solución:

Actualizar inmediatamente a la versión 2.4.51 del Servidor Apache.

Información adicional:

- https://httpd.apache.org/download.cgi
- https://www.bleepingcomputer.com/news/security/apache-fixes-zero-day-vulnerability-exploited-in-the-wild-patch-now/
- https://thehackernews.com/2021/10/new-patch-released-for-actively.html