El fabricante de dispositivos de almacenamiento conectado a la red (NAS) QNAP, dijo este jueves que está investigando su línea por el impacto potencial que surge de dos vulnerabilidades de seguridad que se abordaron en el servidor Apache HTTP el mes pasado.

Las vulnerabilidades críticas, rastreadas como CVE-2022-22721 y CVE-2022-23943, tienen una calificación CVSS de 9.8 e impactan las versiones 2.4.52 y anteriores del Servidor HTTP Apache.

- CVE-2022-22721: Posible desbordamiento de búfer con LimitXMLRequestBody muy grande o ilimitado.
- CVE-2022-23943: Vulnerabilidad de escritura fuera de los límites en mod_sed del servidor Apache HTTP.

Ambas vulnerabilidades, junto con CVE-2022-22719 y CVE-2022-22720, fueron corregidas por los mantenedores del proyecto como parte de la versión 2.4.53, que se envió el 14 de marzo de 2022.

> *«Si bien CVE-2022-22719 y CVE-2022-22720 no afectan a los productos QNAP, CVE-2022-22721 afecta a los modelos QNAP NAS de 32 bits y CVE-2022-23943 afecta a los usuarios que han habilitado mod_sed en Apache HTTP Server en su dispositivo QNAP»,* dijo la compañía en una alerta.

En ausencia de actualizaciones de seguridad fácilmente disponibles, QNAP ha ofrecido soluciones alternativas, que incluyen *«mantener el valor predeterminado '1M' para LimitXMLRequestBody»* y deshabilitar mod_sed, agregando que la función mod_sed está deshabilitada de forma predeterminada en Apache HTTP Server en dispositivos NAS que ejecutan el sistema operativo QTS.

Este aviso llega casi un mes después de que se revelara que se trabaja para resolver una vulnerabilidad de bucle infinito en OpenSSL (CVE-2022-0778, puntaje CVSS: 7.5) y se lanzaran parches para la falla de Dirty Pipe Linux (CVE-2022-0847, puntaje CVSS: 7.8).