QNAP, el fabricante taiwanés de dispositivos de almacenamiento conectado a la red (NAS), lanzó el viernes actualizaciones de seguridad para parchear nueve vulnerabilidades de seguridad, incluyendo un problema crítico que podría explotarse para hacerse cargo de un sistema afectado.

> *«Se informó que una vulnerabilidad afecta a QNAP VS Series NVR que ejecutan QVR. Si se explota, esta vulnerabilidad permite a atacantes remotos ejecutar comandos arbitrarios»*, dijo QNAP.

Rastreada como CVE-2022-27588, con puntaje CVSS de 9.8, la vulnerabilidad se solucionó en QVR 5.1.6 compilación 20220401 y versiones posteriores. El Centro de Coordinación del Equipo de Respuestas a Emergencias Informáticas de Japón (JPCERT/CC) es el responsable de informar sobre la vulnerabilidad.

Aparte de la vulnerabilidad crítica, QNAP también resolvió tres errores de gravedad alta y cinco de gravedad media en su software:

- CVE-2021-38693 (puntaje CVSS de 5.3): Una vulnerabilidad de cruce de ruta en httpd que afecta a los dispositivos QNAP que ejecutan QTS, QuTS hero, QuTScloud y QVR Pro Appliance, lo que lleva a la divulgación de información.
- CVE-2021-44051 (puntaje CVSS de 8.8): Una vulnerabilidad de inyección de comandos en dispositivos QNAP que ejecutan QTS, QuTS hero y QuTScloud, lo que resulta en la ejecución arbitraria de comandos.
- CVE-2021-44052 (puntaje CVSS de 6.5): Una resolución de enlace incorrecta antes del acceso al archivo («seguimiento del enlace»). Vulnerabilidad en dispositivos QNAP que ejecutan QTS, QuTS hero y AuTScloud, lo que permite a los atacantes leer/escribir archivos en ubicaciones de archivos arbitrarias.
- CVE-2021-44053 (puntaje CVSS de 5.7): Una vulnerabilidad de secuencias de comandos en sitios cruzados (XSS) en dispositivos QNAP que ejecutan QTS, QuTS hero y QuTScloud, lo que lleva a la inyección de código.
- CVE-2021-44054 (puntaje CVSS de 4.3): Una vulnerabilidad de redirección abierta en

dispositivos QNAP que ejecutan QTS, QuTS hero y QuTScloud, lo que permite redirigir a los usuarios a páginas web no autorizadas.

- CVE-2021-44055 (puntaje CVSS de 5.3): Una vulnerabilidad de autorización faltante en los dispositivos QNAP que ejecutan Video Station, lo que permite a los atacantes acceder a los datos o realizar acciones no autorizadas.
- CVE-2021-44056 (puntaje CVSS de 7.1): Una vulnerabilidad de autenticación incorrecta en los dispositivos QNAP que ejecutan Video Station, lo que compromete el sistema.
- CVE-2021-44057 (puntaje CVSS de 7.1): Una vulnerabilidad de autenticación incorrecta e los dispositivos QNAP que ejecutan Photo Station, lo que compromete el sistema.