



La vulnerabilidad de Linux Dirty Pipe afecta a una amplia gama de dispositivos NAS de QNAP

El fabricante de dispositivos de almacenamiento conectado a la red (NAS) QNAP, advirtió este lunes sobre una vulnerabilidad de Linux recientemente revelada que afecta a sus dispositivos y que podría ser abusada para elevar los privilegios y obtener el control de los sistemas afectados.

«Se informó que una vulnerabilidad de escalada de privilegios locales, también conocida como Dirty Pipe, afecta el kernel de Linux en el NAS de QNAP que ejecuta QTS 5.0.x y QuTS hero h5.0.x. Si se explota, esta vulnerabilidad permite que un usuario sin privilegios obtenga privilegios de administrador e inyecte código malicioso», [dijo la compañía](#).

La compañía taiwanesa dijo que sigue investigando a fondo su línea de productos en busca de la vulnerabilidad y que los dispositivos NAS de QNAP que ejecutan las versiones 4.x de QTS son inmunes a la vulnerabilidad Dirty Pipe.

Rastreada como CVE-2022-0847 y con puntaje CVSS de 7.8, la vulnerabilidad reside en el kernel de Linux que podría permitir que un atacante sobrescriba datos arbitrarios en cualquier archivo de solo lectura y permitir una toma de control completa de las máquinas vulnerables.

Desde entonces, el problema se solucionó en las versiones de Linux 5.16.11, 5.15.25 y 5.10.102 a partir del 23 de febrero de 2022, tres días después de que se informara al equipo de seguridad del kernel de Linux.

«Actualmente no hay mitigación disponible para esta vulnerabilidad. Recomendamos a los usuarios que vuelvan a consultar e instalen las actualizaciones de seguridad tan pronto como estén disponibles», dijo la compañía.