BOLETÍN DE ALERTA

Boletín Nro.: 2023-44
Fecha de publicación: 19/09/2023
Tema: Vulnerabilidades de inyección de comandos y denegación de servicio (*DoS*) en productos QNAP

Los softwares afectados son:

- QTS, versiones 5.0.1 y 4.5.4.
- QuTS hero, versiones h5.0.1 y h4.5.4.
- QuTScloud, versión c5.0.1.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre cinco vulnerabilidades que afectan a productos QNAP, que permitirían a un atacante autenticado realizar inyección de comandos, denegación de servicio (*DoS*) entre otros.

Las vulnerabilidades corregidas se componen de 1 (una) de severidad "Alta" y 4 (cuatro) de severidad "Media". Las principales se detallan a continuación:

- CVE-2023-23362, de severidad "Alta" y sin puntuación asignada aún. Esta vulnerabilidad de *Command Injection* se debe a una falla de validación de datos de entrada en los sistemas QTS, QuTS hero y QuTScloud de QNAP. Esto permitiría a un actor malicioso autenticado, realizar ejecución de comandos arbitrarios en el sistema afectado de forma remota.

- CVE-2023-23358 y CVE-2023-23359, ambas de severidad "Media" y sin puntuación asignada aún. Estas vulnerabilidades de escritura fuera de los límites se deben a un error en los punteros *NULL* de los sistemas operativos para QTS, QuTS hero y QuTScloud de QNAP. Esto permitiría a un actor malicioso autenticado provocar un ataque de denegación de servicio (*DoS*) en el sistema afectado de forma remota.

Se puede acceder al listado completo de vulnerabilidades aquí

Impacto:

La explotación exitosa de estas vulnerabilidades podría permitir a un actor malicioso autenticado realizar ejecución de comandos arbitrarios, denegación de servicio (*DoS*), entre otros.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante a través de la siguiente guía:

- https://www.qnap.com/go/download

Información adicional:

- https://securityonline.info/qnap-rolls-out-critical-security-updates/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23362
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23358
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23359
- https://www.qnap.com/en/security-advisories?ref=security_advisory_details
- https://www.qnap.com/en/security-advisory/qsa-23-18
- https://www.qnap.com/en/security-advisory/qsa-23-19
- https://www.qnap.com/en/security-advisory/qsa-23-21
- https://www.qnap.com/go/download