Vulnerabilidades en productos QNAP

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

Qnap ha publicado un aviso de seguridad para tratar **3 vulnerabilidades**, **1** de **severidad crítica**, cuyo identificador es CVE-2024-21899 , así como **dos de severidad media** cuyos identificadores son CVE-2024-21900 y CVE-2024-21901. Los errores afectan a los productos **QTS, QuTS hero, QuTScloud y myQNAPcloud**.

La explotación de la vulnerabilidad crítica podría suponer un compromiso para la seguridad del sistema vía red con impacto en la confidencialidad, integridad y disponibilidad de los sistemas que se vean afectados.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir esta y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

Los productos afectados son los siguientes:

- QTS 5.1.x.
- QTS 4.5.x.
- QuTS hero h5.1.x.
- QuTS hero h4.5.x.
- QuTScloud c5.x.
- myQNAPcloud 1.0.

3. Análisis técnico

Los detalles de la vulnerabilidad crítica tratada en este aviso son los siguientes:

CVE-2024-21899: vulnerabilidad de autenticación incorrecta que afecta a varias versiones del sistema operativo QNAP. La explotación de esta vulnerabilidad podría permitir a agentes maliciosos comprometer la seguridad del sistema a través de la red.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-287: Improper Authentication

CVSS Base: **9.8**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: Baja
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

4. Mitigación / Solución

QNAP recomienda actualizar regularmente sistema y aplicaciones a la última versión para beneficiarse de las correcciones de estas vulnerabilidades.

Las formas de actualizar las herramientas afectadas por estas vulnerabilidades se encuentran disponibles dentro del propio aviso, que son las siguientes:

- QTS 5.1.x, actualizar a la versión QTS 5.1.3.2578 compilación 20231110 y posteriores.
- QTS 4.5.x, actualizar a la versión QTS 4.5.4.2627 compilación 20231225 y posteriores.
- QuTS hero h5.1.x, actualizar a la versión QuTS hero h5.1.3.2578 compilación 20231110 y posteriores.
- QuTS hero h4.5.x, actualizar a la versión QuTS hero h4.5.4.2626 compilación 20231225 y posteriores.
- QuTScloud c5.x, actualizar a la versión QuTScloud c5.1.5.265 y posteriores.
- myQNAPcloud 1.0.x, actualizar a la versión myQNAPcloud 1.0.52 (2023/11/24) y posterior.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-21899.
- CVE-2024-21900.
- CVE-2024-21901.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY