Alerta de seguridad cibernética	9VSA24-00953-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	15 de enero de 2024
Última revisión	15 de enero de 2024

NOTIFICACIÓN: La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de una vulnerabilidad parchada por QNAP para varios de sus productos.

Vulnerabilidades

CVE-2023-39296
CVE-2022-43634
CVE-2023-41287
CVE-2023-41288
CVE-2023-47559
CVE-2023-47560

Impacto

Vulnerabilidades de riesgo alto:

CVE-2023-39296: Vulnerabilidad de contaminación de prototipos que, de ser explotada, podría permitir a usuarios remotos el invalidar los atributos existentes con otros de tipo incompatible, lo que puede provocar que el sistema colapse.

CVE-2023-47559: Vulnerabilidad XSS que podría permitir a usuarios autenticado el inyectar código malicioso a través de internet.

CVE-2023-47560: Vulnerabilidad de OS commnand injection podría permitir a usuarios autenticados a ejecutar comandos a través de una red.

Productos afectados

CVE-2023-39296: QTS versiones 5.1.x y QuTS hero versiones h5.1.x. Parchado en QTS 5.1.3.2578 build 20231110 y QuTS hero h5.1.3.2578 build 20231110.

CVE-2023-47559 y CVE-2023-47560: QuMagie 2.2.x. Parchado en QuMagie 2.2.1 y posterior.

Enlaces

https://www.qnap.com/en/security-advisory/qsa-23-64
https://www.qnap.com/en/security-advisory/qsa-23-23
https://www.qnap.com/en/security-advisories

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.15 16:43:21 -03'00'