Alerta de seguridad cibernética	9VSA23-00779-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 de enero de 2023

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 sobre una vulnerabilidad crítica que afecta a QNAP NAS, para la que la empresa liberó un parche.

Vulnerabilidades

CVE-2022-27596

Impacto

Vulnerabilidades de riesgo crítico
CVE-2022-27596: Si es explotada, esta vulnerabilidad permite a un atacante remoto inyectar código malicioso.

Mitigación
Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados
QTS 5.0.1 y QuTS hero h5.0.1

Enlaces
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27596
https://www.qnap.com/en/security-advisory/qsa-23-01

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.01.31 12:38:36 -03'00'

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO
https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob