Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00416-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de abril de 2021
Última revisión	05 de abril de 2021

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 equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información sobre dos vulnerabilidades críticas en aparatos NAS de la marca QNAP QTS.

De acuerdo con QNAP, la vulnerabilidad ha sido corregida en sus modelos más nuevos, que corren QTS 4.5, pero que trabajarán en un parche para sus modelos que usan versiones anteriores a la 4.5, la que deberían liberar en las próximas semanas.

Vulnerabilidades

Ambas vulnerabilidades carecen aún de CVE.

Impactos

Las vulnerabilidades críticas descritas son dos:

Una permite a un atacante remoto con acceso al servidor web (puerto por default 8080) ejecutar comandos shell arbitrarios sin previo conocimiento de las credenciales web.

La otra permite a un atacante remoto con acceso al servidor DLNA (puerto por default 8200) crear datos de archivo arbitrarios en cualquier ubicación no existente, sin previo conocimiento de las credenciales. Puede también ser elevado para ejecutar comandos arbitrarios al NAS remoto.

Productos Afectados

QNAP QTS con sistemas anteriores a la versión 4.5.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor cuando estén disponibles.

Enlaces

https://www.qnap.com/en/security-advisories/

https://securingsam[.]com/new-vulnerabilities-allow-complete-takeover/

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.05 13:25:24 -04'00'