BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-60
Fecha de publicación: 30/10/2024
Tema: Vulnerabilidad Zero-Day en software de respaldo de QNAP
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Dispositivo NAS TS-454 con SO HBS 3 Hybrid Backup Sync versiones 25.1.x y anteriores
- Servicio SMB de QNAP NAS: versiones 4.15.x y anteriores

Descripción

QNAP ha identificado un par de vulnerabilidades zero-day, conocidas como CVE-2024-50387 y CVE-2024-50388, demostradas en el evento Pwn2Own, ambas permiten la **ejecución remota de código (RCE),** mediante inyección SQL e inyección de comandos de sistema operativo respectivamente, lo cual significa que un atacante puede ejecutar comandos en el dispositivo vulnerable desde una ubicación remota. Esto puede ser realizado mediante la inyección de código y aprovechando permisos o configuraciones insuficientes en el manejo de las solicitudes hacia el servidor de respaldo. Esta clase de vulnerabilidad pone en riesgo la integridad de los datos almacenados en el NAS, permitiendo potencialmente el acceso o el control total de los archivos y configuraciones.

Detalles Técnicos CVE-2024-50387:

- **Tipo de Vulnerabilidad:** Inyección SQL (SQLi).
- **Componente Afectado:** Servicio SMB en dispositivos QNAP NAS.
- **Impacto:** Ejecución de comandos arbitrarios con privilegios de root, lo que permite al atacante tomar control total del dispositivo afectado

Detalles Técnicos CVE-2024-50388:

- **Tipo de Vulnerabilidad:** Inyección de comandos del sistema operativo.
- **Componente Afectado:** HBS 3 Hybrid Backup Sync versión 25.1.x.
- **Impacto:** Ejecución remota de comandos, lo que podría otorgar al atacante control total sobre el dispositivo NAS.

Solución

Para solucionar esta vulnerabilidad, QNAP ha lanzado los parches de seguridad que corrigen estas vulnerabilidades en los siguientes enlaces: Vulnerability in SMB Service (PWN2OWN 2024) - Security Advisory | QNAP y Vulnerability in HBS 3 Hybrid Backup Sync (PWN2OWN 2024) - Security Advisory | QNAP

Se recomienda a los usuarios actualizar el servicio SMB a la versión 4.15.002 o posterior y a la versión HSB 3 Hybrid Backup Sync 25.11.673 o posterior para mitigar el riesgo de explotación.

Información adicional:

- QNAP fixes NAS backup software zero-day exploited at Pwn2Own
- Vulnerability in HBS 3 Hybrid Backup Sync (PWN2OWN 2024) - Security Advisory | QNAP
- Vulnerability in SMB Service (PWN2OWN 2024) - Security Advisory | QNAP

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com