Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

TETÃ REKUÁI GOBIERNO NACIONAL

BOLETÍN DE ALERTA

Boletín Nro.: 2021-09

Fecha de publicación: 23/04/2021

Tema: Explotación masiva de Vulnerabilidad crítica en dispositivos Qnap

Dispositivos afectados:

- Todas las versiones de QNAP NAS están afectadas por al menos una de las vulnerabilidades.
- Complementos:
    - QNAP NAS ejecutando Multimedia Console o el Media Streaming add-on
    - QNAP NAS ejecutando HBS 3 Hybrid Backup Sync

Descripción

Se han descubierto 3 vulnerabilidades críticas de Día 0 (Zero-Day) en los dispositivos QNAP. Investigadores externos encontraron una vulnerabilidad crítica (CVE-2021-28799) que permite a los atacantes iniciar sesión en dispositivos NAS (almacenamiento conectado a la red) de QNAP. Las otras dos vulnerabilidades afectan al servidor web (CVE-2020-2509) y al servidor DLNA (CVE-2020-36195) del NAS.

Para poner en contexto al lector aclaramos que DLNA (Digital Living Network Alliance) es una tecnología presente en muchos equipos electrónicos como televisores, smartphones, consolas, discos duros, tablets, etc a través de la cual todos ellos se pueden interconectar con el fin de compartir contenido entre ellos mismos.

Dos de las vulnerabilidades son de explotación remota (CVE-2020-36195 y CVE-2020-36195) y permiten la ejecución de código remoto. Una de las vulnerabilidades permite acceso total al dispositivo a través de una cuenta "backdoor" códificada (CVE-2021-28799). Existe evidencia de que las 3 vulnerabilidades están siendo explotadas activamente en conjunto en el marco de ataques dirigidos y dentro de campañas de ransomware. A continuación, se detallan las vulnerabilidades:

- CVE-2021-28799: permite a un atacante utilizar credenciales codificadas.
- CVE-2020-36195: permite a un atacante remoto con acceso al servidor web (puerto predeterminado 8080) ejecutar comandos de shell arbitrarios, sin conocimiento previo de las credenciales web.

- CVE-2020-36195: permite a un atacante remoto con acceso al servidor DLNA (puerto predeterminado 8200) crear datos de archivos arbitrarios en cualquier ubicación (no existente), sin ningún conocimiento o credenciales previas. También se puede elevar para ejecutar comandos arbitrarios en el NAS remoto.

Actualmente existe una campaña masiva de ataque a estos dispositivos utilizando un ransomware llamado Qlocker el cual utiliza 7zip para cifrar dispositivos QNAP. Dicho ransomware está utilizando las tres vulnerabilidades reportadas para explotar los dispositivos QNAP y propagarse. Es crítico que realice las actualizaciones de sus dispositivos para evitar ser comprometidos.

QNAP ha publicado las actualizaciones de firmware correspondientes para las siguientes versiones:

- QTS 4.2.6 Build 20210327 y siguientes
- QTS 4.3.3.1624, 4.3.4.1632, 4.3.6.1620 y después; también HBS 3 Hybrid Backup Sync 3.0.210412 y los siguientes; además Media Streaming add-on 430.1.8.8 y los siguientes en dichos QTS.
- QTS 4.4.x and later: Multimedia Console 1.3.4 and later
- QTS 4.5.1.1495, 4.5.2.1566 y posteriores además también HBS 3 Hybrid Backup Sync 16.0.0415 y siguientes en dicho QTS.
- QTS 4.5.2.1566, 4.5.1.1495 y posteriores
- QuTS hero h4.5.1.1491 build 20201119 y siguiente y también HBS 3 Hybrid Backup Sync 16.0.0419 y siguientes.
- QuTScloud c4.5.1~c4.5.4: HBS 3 Hybrid Backup Sync 16.0.0419 y siguientes.

Si la versión del sistema operativo de su NAS no figura en la lista puede consultar las páginas oficiales de QNAS en busca de actualizaciones.

Impacto:

La explotación de algunas de las 3 vulnerabilidades mencionadas puede derivar en el control total del dispositivo QNAS por parte de un atacante remoto no autenticado. En el caso de ser afectado por el ransomware QLocker, puede derivar en la pérdida total de los archivos almacenados en el dispositivo.

Solución y prevención

- Se recomienda bloquear los accesos externos desde el internet a los dispositivos si no son necesarios y/o hasta que se actualicen los mismos.
- Instale las actualizaciones de Firmware publicadas por QNAS
    - CVE-2021-28799 y CVE-2020-2509
        - Inicie sesión en QTS o QuTS hero como administrador.
        - Vaya a **Panel de control (Control Panel) > Sistema (System) > Actualización de firmware (Firmware Update).**
        - En **Actualización en vivo (Live Update)**, haga clic en **Buscar actualizaciones (Check for Update.)**.
        - QTS o QuTS hero descarga e instala la última actualización disponible.
        - **Nota:** También puede descargar la actualización desde el sitio web de QNAP. **Vaya a Soporte** (**Support**) **> Centro de descargas** (**Download Center**) y luego realice una actualización manual para su dispositivo específico.
    - CVE-2020-36195 - Actualización del complemento de transmisión de medios
        - Inicie sesión en QTS como administrador.
        - Abra el **App Center** y luego haga clic en la **lupa** . Aparecerá un cuadro de búsqueda.
        - Escriba “Media Streaming add-on” y luego presione **ENTER**. El complemento Media Streaming aparece en los resultados de la búsqueda.
        - Haga clic en Actualizar (**Update**). Aparecerá un mensaje de confirmación. **Nota**: Si el botón Actualizar (Update) no está disponible significa que su complemento Media Streaming ya está actualizado.
        - Haga clic en Aceptar (**OK**).
        - La aplicación está actualizada.

Referencias

- https://www.qnap.com/en/security-advisory/qsa-21-05
- https://www.qnap.com/en/security-advisory/qsa-21-11
- https://www.qnap.com/en/security-advisory/QSA-21-13
- https://www.bleepingcomputer.com/news/security/qnap-removes-backdoor-account-in-nas-backup-disaster-recovery-app/
- https://www.bleepingcomputer.com/news/security/massive-qlocker-ransomware-attack-uses-7zip-to-encrypt-qnap-devices/
- https://portswigger.net/daily-swig/qnap-fixes-critical-rce-vulnerabilities-in-nas-devices
- https://securingsam.com/new-vulnerabilities-allow-complete-takeover/