El fabricante taiwanés de dispositivos de almacenamiento en red (NAS) Synology ha corregido una vulnerabilidad crítica de seguridad en sus sistemas DiskStation y BeePhotos, que podría permitir la ejecución remota de código.

Conocida como CVE-2024-10443 y llamada RISK:STATION por la empresa Midnight Blue, esta vulnerabilidad de día cero fue demostrada en el concurso de hacking Pwn2Own Irlanda 2024 por el investigador de seguridad Rick de Jager.

> RISK:STATION es una *«vulnerabilidad zero-click sin autenticación que permite a los atacantes ejecutar código con privilegios de root en los populares dispositivos NAS Synology DiskStation y BeeStation, afectando a millones de dispositivos»*, explicó la empresa holandesa.

La característica zero-click de la vulnerabilidad implica que no requiere ninguna acción del usuario para ser explotada, lo cual permite a los atacantes acceder a los dispositivos, robar información confidencial e instalar malware adicional.

Las versiones afectadas por la vulnerabilidad son:

- BeePhotos para BeeStation OS 1.0 (actualización requerida a la versión 1.0.2-10026 o superior)
- BeePhotos para BeeStation OS 1.1 (actualización requerida a la versión 1.1.0-10053 o superior)
- Synology Photos 1.6 para DSM 7.2 (actualización requerida a la versión 1.6.2-0720 o superior)
- Synology Photos 1.7 para DSM 7.2 (actualización requerida a la versión 1.7.0-0795 o superior)

Por el momento, se han retenido detalles técnicos adicionales sobre la vulnerabilidad para brindar tiempo suficiente a los clientes para aplicar los parches necesarios. Midnight Blue estimó que entre uno y dos millones de dispositivos Synology están afectados y expuestos a

internet.

QNAP Resuelve 3 Fallos Críticos

Esta revelación coincide con la solución de tres vulnerabilidades críticas en dispositivos de QNAP que afectan a QuRouter, el servicio SMB y HBS 3 Hybrid Backup Sync, todas explotadas en el evento Pwn2Own:

- CVE-2024-50389: Resuelto en QuRouter versión 2.4.5.032 y posteriores
- CVE-2024-50387: Corregido en el servicio SMB en versiones 4.15.002 y h4.15.002 y posteriores
- CVE-2024-50388: Corregido en HBS 3 Hybrid Backup Sync en la versión 25.1.1.673 y posteriores

Aunque no existen indicios de que estas vulnerabilidades hayan sido explotadas en escenarios reales, se recomienda a los usuarios aplicar los parches lo antes posible, ya que los dispositivos NAS han sido objetivos frecuentes de ataques de ransomware.