Synology publicó actualizaciones de seguridad para corregir una vulnerabilidad crítica que afecta al servidor VPN Plus, que podría explotarse para hacerse cargo de los sistemas afectados.

Rastreada como CVE-2022-43931, la vulnerabilidad tiene una clasificación de gravedad máxima de 10 en la escala CVSS y se describió como un error de escritura fuera de los límites en la funcionalidad de escritorio remoto en Synology VPN Plus Server.

La explotación exitosa del problema *«permite a los atacantes remotos ejecutar comandos arbitrarios a través de vectores no especificados»*, dijo la compañía taiwanesa y agregó que fue descubierto internamente por su Equipo de Respuesta a Incidentes de Seguridad del Producto (PSIRT).

Se recomienda a los usuarios de VPN Plus Server para Synology Router Manager (SRM) 1.2 y VPN Plus Server para SRM 1.3 que actualicen a las versiones 1.4.3-0534 y 1.4.4-0635, respectivamente.

El fabricante de dispositivos de almacenamiento conectado a la red, en un segundo aviso, también advirtió sobre varias vulnerabilidades en SRM que podrían permitir a atacantes remotos ejecutar comandos arbitrarios, realizar ataques de denegación de servicio o leer archivos arbitrarios.

Se han retenido los detalles exactos sobre las vulnerabilidades, y se insta a los usuarios a actualizar a las versiones 1.2.5-8227-6 y 1.3.1-9346-3 para mitigar las posibles amenazas.

Gaurav Barauah, Lukas Kupczyk de CrowdStrike, el investigador de DEVCORE, Orange Tsai y la firma de seguridad de TI con sede en los Países Bajos, Computest, fueron acreditados por informar las vulnerabilidades.

Cabe mencionar que algunas de las vulnerabilidades se demostraron en el concurso Pwn20wn 2022 realizado entre el 6 y el 9 de diciembre de 2022 en Toronto.

Baruah ganó $20,000 dólares por un ataque de inyección de comandos contra la interfaz WAN de Synology RT6600ax, mientras que Computest ganó 5,000 dólares por un exploit shell raíz de inyección de comandos dirigido a su interfaz LAN.