El fabricante de equipos de red Zyxel lanzó parches de seguridad para una vulnerabilidad crítica que afecta a sus dispositivos de almacenamiento conectado a la red (NAS).

Rastreada como CVE-2022-34747 (puntuación CVSS: 9.8), la vulnerabilidad se relaciona con una falla *«de cadena de formato»* que afecta a los modelos NAS326, NAS540 y NAS542. Zyxel se dio crédito al investigador Shaposhnikov Ilya por informar la falla.

> *«Se encontró una vulnerabilidad de cadena de formato en un binario específico de producto Zyxel NAS que podría permitir a un atacante lograr la ejecución remota no autorizada de código a través de un paquete UDP manipulado»*, dijo la compañía en un aviso el 6 de septiembre.

La vulnerabilidad afecta a las siguientes versiones:

- NAS326 (V5.21 (AAZF.11) C0 y anterior)
- NAS540 (V5.21(AATB.8)C0 y anterior)
- NAS542 (V5.21(ABAG.8)C0 y anterior)

La divulgación se produce cuando Zyxel abordó previamente la escalada de privilegios locales y las vulnerabilidades de cruce de directorios autenticados (CVE-2022-30526 y CVE-2022-2030) que afectaron a sus productos de firewall en julio.

Hackear dispositivos NAS se está convirtiendo en una práctica cada vez más común. Si no se toman las precauciones necesarias o no se mantiene el software actualizado, los atacantes pueden robar datos confidenciales y personales. En algunos casos, incluso logran eliminar datos permanentemente.

En junio de 2022, también se solucionó una vulnerabilidad de seguridad (CVE-2022-0823) que dejaba a los switches de la serie GS1200 susceptibles a ataques de adivinación de contraseñas por medio de un ataque de canal lateral de tiempo.