Investigadores de seguridad cibernética revelaron detalles de vulnerabilidades de seguridad críticas en los dispositivos de almacenamiento conectado a la red (TNAS), de TerraMaster, que podrían encadenarse para lograr la ejecución remota de código no autenticado con los privilegios más altos.

Los problemas residen en TOS, una abreviatura de TerraMaster Operating System, y *«puede otorgar acceso a los atacantes no autenticados a la caja de la víctima simplemente conociendo la dirección IP»*, dijo Paulos Yibelo, de la compañía de seguridad Octagon Networks.

TOS es el sistema operativo diseñado para dispositivos TNAS, que permite a los usuarios administrar el almacenamiento, instalar aplicaciones y hacer copias de seguridad de los datos. Después de la divulgación responsable, las vulnerabilidades se corrigieron en la versión 4.2.30 de TOS, lanzada el 1 de marzo de 2022.

Una de las vulnerabilidades, rastreada como CVE-2022-24990, se refiere a un caso de fuga de información en un componente llamado *«webNasIPS»,* que resultó en la exposición de la versión de firmware de TOS, la dirección IP y MAC de la interfaz de puerta de enlace predeterminada y un hash de la contraseña de administrador.

La segunda falla, se relaciona con una vulnerabilidad de inyección de comandos en un módulo PHP llamado *«createRaid»* (CVE-2022-24989), lo que resulta en un escenario donde los dos problemas se pueden unir para enviar un comando especialmente diseñado para lograr la ejecución remota de código.

> *«En general, este fue un proyecto muy interesante. Hemos utilizado múltiples componentes de una fuga de información, junto con otra fuga de información del tiempo de la máquina, y la hemos encadenado con una inyección de comando de sistema operativo autenticado para lograr la ejecución remota de código no autenticado como root»,* dijo Yibelo.

La divulgación llega cuando los dispositivos TerraMaster NAS también han sido objeto de ataques de ransomware Deadbolt, uniéndose a QNAP y ASUSTOR, y la compañía dijo que abordó las vulnerabilidades que probablemente fueron explotadas por los hackers para implementar el ransomware en la versión 4.2.30 de TOS.

Aún no está claro si el mismo conjunto de vulnerabilidades descubiertas por Octagon Networks se utilizó como arma para las infecciones de Deadbolt.

«Se corrigió una vulnerabilidad de seguridad relacionada con el ataque de ransomware Deadbolt», dijo la compañía, además de recomendar a los usuarios que *«reinstalen la última versión del sistema TOS (4.2.30 o posterior) para evitar que los archivos sin cifrar sigan encriptados».*