Basque CyberSecurity Centre

Vulnerabilidad en dispositivos de almacenamiento (NAS) de Zyxel

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Aviso de seguridad

Zyxel ha publicado un aviso de seguridad en la que se corrige una vulnerabilidad que afecta a algunos dispositivos de almacenamiento conectados en red (NAS). Los modelos en cuestión son Zyxel NAS326, NAS540 y NAS542. El error, de severidad alta, cuenta con el identificador CVE-2023-27988 y podría producir una condición de inyección de comandos del sistema operativo de forma remota. Su explotación implica un alto impacto en la confidencialidad, integridad y disponibilidad de los sistemas.

El fabricante ya ha publicado las actualizaciones correspondientes corrigiendo de esta manera el fallo destacado, por lo que, para prevenir estas y otras vulnerabilidades, se recomienda mantener siempre actualizados los sistemas y aplicaciones.

2. Recursos afectados

- Zyxel NAS326 versión V5.21(AAZF.12)C0 y anteriores.
- Zyxel NAS540 versión V5.21(AATB.9)C0 y anteriores.
- Zyxel NAS542 versión V5.21(ABAG.9)C0 y anteriores.

3. Análisis técnico

Los detalles de la vulnerabilidad tratada en este aviso son los siguientes:

CVE-2023-27988: vulnerabilidad de inyección de comando posterior a la autenticación que podría permitir que un atacante autenticado, con privilegios de administrador, ejecute algunos comandos del sistema operativo en un dispositivo afectado de forma remota.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)

CVSS Base: 7.2

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

4. Mitigación / Solución

Para la mitigación de esta vulnerabilidad, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para corregir el fallo tratado en este aviso, Zyxel ha publicado actualizaciones de firmware para los modelos afectados, que se encuentran disponibles en los siguientes enlaces:

- Actualización para dispositivo Zyxel NAS326.
- Actualización para dispositivo Zyxel NAS540.
- La actualización para los dispositivos Zyxel NAS542 se encuentra disponible como descarga directa dentro del propio aviso.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2023-27988.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA