# Vulnerabilidades en productos NAS de Zyxel

CYBERZAINTZA-AVISOS

**TLP: CLEAR**

www.ciberseguridad.eus

Tabla de contenido

Sobre el BCSC....3
1. Resumen ejecutivo....4
2. Recursos afectados....5
3. Análisis técnico....6
4. Mitigación / Solución....9
5. Referencias Adicionales....10

## 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. Resumen ejecutivo

Zyxel ha publicado un aviso de seguridad en el que se tratan un total de 6 vulnerabilidades, de omisión de autenticación e inyección de comandos, que afectan a productos NAS del fabricante. Tres de ellas cuentan con una severidad crítica, CVE-2023-35138, CVE-2023-4473 y CVE-2023-4474, mientras que el resto, CVE-2023-35137, CVE-2023-37927, CVE-2023-37928, han sido catalogadas con severidad alta. La mayoría de estos fallos, de ser aprovechados, supondrían una amenaza de alta gravedad para la confidencialidad, disponibilidad e integridad de los sistemas.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

## 2. Recursos afectados

- Zyxel NAS326 versiones V5.21(AAZF.14)C0 y anteriores.
- Zyxel NAS542 versiones V5.21(ABAG.11)C0 y anteriores.

## 3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en este aviso son los siguientes:

CVE-2023-35138: vulnerabilidad de inyección de comandos en la función *show_zysync_server_contents* de la versión de firmware V5.21(AAZF.14)C0 de Zyxel NAS326 y la versión de firmware NAS542 V5.21(ABAG.11)C0, que podría permitir que un atacante no autenticado ejecute comandos del sistema operativo enviando una solicitud HTTP POST diseñada.

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: **9.8**

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

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

CVE-2023-4473: vulnerabilidad de inyección de comandos en el servidor web de la versión de firmware V5.21(AAZF.14)C0 de Zyxel NAS326 y la versión de firmware NAS542 V5.21(ABAG.11)C0, que podría permitir que un atacante no autenticado ejecute algunos comandos del sistema operativo enviando una URL diseñada a un dispositivo vulnerable.

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: **9.8**

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Bajos**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**

- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-4474: vulnerabilidad de neutralización inadecuada de elementos especiales en el servidor WSGI del firmware Zyxel NAS326 versión V5.21(AAZF.14)C0 y NAS542 versión V5.21(ABAG.11)C0, que podría permitir que un atacante no autenticado ejecute algunos comandos del sistema operativo enviando una URL diseñada a un dispositivo vulnerable.

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: **9.8**

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

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

CVE-2023-37927: vulnerabilidad de neutralización inadecuada de elementos especiales en el programa CGI del firmware Zyxel NAS326 versión V5.21(AAZF.14)C0 y NAS542 versión V5.21(ABAG.11)C0, que podría permitir que un atacante autenticado ejecute algún comando del sistema operativo enviando una URL diseñada a un dispositivo vulnerable.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 287: Improper Authentication

CVSS Base: **8.8**

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

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

CVE-2023-37928: vulnerabilidad de inyección de comando posterior a la autenticación en el servidor WSGI de la versión de firmware V5.21(AAZF.14)C0 de Zyxel NAS326 y la versión de firmware NAS542 V5.21(ABAG.11)C0, que podría permitir que un atacante autenticado ejecute comandos del sistema operativo enviando una URL diseñada a un dispositivo vulnerable.

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: **8.8**

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

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

CVE-2023-35137: vulnerabilidad de autenticación incorrecta en el módulo de autenticación de la versión de firmware V5.21(AAZF.14)C0 de Zyxel NAS326 y la versión de firmware NAS542 V5.21(ABAG.11)C0, que podría permitir que un atacante no autenticado obtenga información del sistema enviando una URL manipulada. a un dispositivo vulnerable.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 287: Improper Authentication

CVSS Base: **7.5**

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

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

## 4. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para corregir estas vulnerabilidades, Zyxel recomienda aplicar las actualizaciones de seguridad aportadas para cada producto disponibles para su descarga desde el propio aviso.

## 5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2023-35138.
- CVE-2023-4473.
- CVE-2023-4474.
- CVE-2023-37927.
- CVE-2023-37928.
- CVE-2023-35137.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY