Basque CyberSecurity Centre

Vulnerabilidades en Zyxel firmware NR7101 (CVE-2022-43389, CVE-2022-43390, CVE-2022-43391, CVE-2022-43392)

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 donde se reportan 4 vulnerabilidades de inyección de comandos y desbordamiento de búfer de CPE, ONT de fibra y extensores WiFi. Los fallos CVE-2022-43389, CVE-2022-43391, CVE-2022-43392, cuentan con una severidad alta y el restante, CVE-2022-43390, media.

El impacto principal que producen estas vulnerabilidades, de no ser actualizadas, se corresponde con la perdida de disponibilidad de los componentes afectados, si se diese una explotación exitosa de las mismas.

2. Recursos afectados

- Productos bajo el firmware NR7101 en versiones anteriores a la V1.15 (ACCC.3) C0

3. Análisis técnico

El detalle de las vulnerabilidades tratadas es el siguiente:

CVE-2022-43389: vulnerabilidad de desbordamiento de búfer en la biblioteca del servidor web en el firmware Zyxel NR7101 y versiones anteriores a V1.15 (ACCC.3) C0, que podría permitir que un atacante no autenticado ejecute algunos comandos del sistema operativo o provoque condiciones de denegación de servicio (DoS) en un dispositivo vulnerable.

La métrica de la vulnerabilidad es la siguiente:

CVSS Base: 8.6, alta

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

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

CVE-2022-43391: vulnerabilidad de desbordamiento de búfer en el parámetro del programa CGI en el firmware Zyxel NR7101 anterior a V1.15 (ACCC.3) C0, que podría permitir que un atacante autenticado provoque condiciones de denegación de servicio (DoS) mediante el envío de una solicitud HTTP manipulada.

La métrica de la vulnerabilidad es la siguiente:

CVSS Base: 7.1, alta

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

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

CVE-2022-43392: vulnerabilidad de desbordamiento de búfer en el parámetro del servidor web en el firmware Zyxel NR7101 anterior a V1.15 (ACCC.3) C0, que podría permitir que un atacante autenticado provoque condiciones de

denegación de servicio (DoS) mediante el envío de una solicitud de autorización manipulada.

La métrica de la vulnerabilidad es la siguiente:

CVSS Base: 7.1, alta

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

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

CVE-2022-43390: vulnerabilidad de inyección de comandos en el programa CGI del firmware Zyxel NR7101 anterior a V1.15 (ACCC.3) C0, que podría permitir que un atacante autenticado ejecute algunos comandos del sistema operativo en un dispositivo vulnerable mediante el envío de una solicitud HTTP manipulada.

La métrica de la vulnerabilidad es la siguiente:

CVSS Base: 5.4, media

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

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

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Desde Zyxel se aconseja a los usuarios que instalen las actualizaciones de firmware correspondientes, cuya lista se puede consultar en la nota de seguridad, para obtener una protección óptima. También se señala que para los productos que no dispongan de enlace de descarga, los clientes deben comunicarse con el equipo de soporte local de Zyxel para obtener el archivo. Por último, se informa que los usuarios finales que recibieron su dispositivo Zyxel proveniente de un ISP, se recomienda que se comuniquen directamente con el equipo de soporte del ISP, ya que el dispositivo puede tener configuraciones personalizadas.

5. Referencias Adicionales

- Aviso de seguridad de Zyxel
- CVE-2022-43389
- CVE-2022-43391
- CVE-2022-43392
- CVE-2022-43390

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA