Basque CyberSecurity Centre

Vulnerabilidades críticas en firewalls ZyWall 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 una guía que proporciona orientación y recomendaciones sobre cómo abordar y mitigar los problemas relacionados con los recientes ataques a dispositivos ZyWall. Las vulnerabilidades que los atacantes están utilizando son CVE-2023-28771, CVE-2023-33009 y CVE-2023-33010. La explotación de estas vulnerabilidades puede llevar a la ejecución remota de código y la denegación de servicio, lo que representa una amenaza significativa para la confidencialidad, integridad y disponibilidad de los sistemas afectados.

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

2. Recursos afectados

Productos afectados	Versiones afectadas para CVE-2023- 28771	Versiones afectadas para CVE-2023- 33009 y CVE-2023-33010
ATP	ZLD versión V4.60 a la V5.35	ZLD versión V4.32 a la V5.36 Patch 1
USG FLEX	ZLD versión V4.60 a la V5.35	ZLD versión V4.50 a la V5.36 Patch 1
USG FLEX50(W) / USG20(W)-VPN	No afecta	ZLD versión V4.25 a la V5.36 Patch 1
VPN	ZLD versión V4.60 a la V5.35	ZLD versión V4.30 a la V5.36 Patch 1
ZyWALL/USG	ZLD versión V4.60 a la V4.73	ZLD versión V4.25 a la V4.73 Patch 1

3. Análisis técnico

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

CVE-2023-28771: vulnerabilidad que produce un manejo incorrecto de mensajes de error en algunas versiones del firewall que podría permitir a un atacante no autenticado ejecutar comandos del sistema operativo de forma remota enviando paquetes manipulados a un dispositivo afectado.

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**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-33009: vulnerabilidad de desbordamiento de búfer en la función de notificación en algunas versiones del firewall que podría permitir a un atacante no autenticado causar condiciones de denegación de servicio (DoS) e incluso ejecutar código de forma remota en un dispositivo afectado.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 120: Buffer Copy without Checking Size of Input (Classic Buffer Overflow)

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**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-33010: vulnerabilidad de desbordamiento de búfer en la función de procesamiento de ID en algunas versiones del firewall que podría permitir a un

atacante no autenticado causar condiciones de DoS e incluso ejecutar código de forma remota en un dispositivo afectado.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 120: Buffer Copy without Checking Size of Input (Classic Buffer Overflow)

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**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

4. Mitigación / Solución

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

Por un lado, Zyxel ha compartido los síntomas que pueden indicar la presencia de dispositivos afectados que son los siguientes:

- El dispositivo deja de responder.
- No se puede acceder a la interfaz de gestión web o SSH del dispositivo.
- Interrupciones en la red.
- Desconexión de las conexiones VPN.

Por otro, para solucionar las vulnerabilidades mencionadas, Zyxel recomienda encarecidamente a los usuarios que instalen la última versión del firmware disponible a través de los canales habituales usados por la compañía (actualización mediante notificaciones push en la interfaz web para dispositivos locales, actualizaciones programadas de firmware para dispositivos basados en la nube), a fin de corregir los fallos y garantizar una protección adecuada. Además, se aconseja seguir las siguientes pautas como medidas temporales de mitigación y precaución:

- Si no es absolutamente necesario administrar los dispositivos desde el lado de la WAN, se recomienda desactivar los servicios de HTTP/HTTPS en la WAN.

Si se necesitase gestionar dispositivos desde el lado de la WAN:

- Habilitar el Control de Políticas y agreguar reglas para permitir el acceso solo desde direcciones IP de origen confiables.
- Habilitar el filtrado de GeoIP para permitir el acceso solo desde ubicaciones confiables.
- Si no se necesita utilizar la función de VPN IPSec, desactivar el puerto UDP 500 y el puerto 4500.

5. Referencias Adicionales

- Guía Zyxel ZyWall.
- CVE-2023-28771.
- CVE-2023-33009.
- CVE-2023-33010.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA