# Vulnerabilidad Zyxel

BCSC-VULNERABILIDAD-ZYXEL

TLP:WHITE

www.basquecybersecurity.eus

Mayo 2022

# 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 Respuesta 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:

# 1. RESUMEN EJECUTIVO

El equipo de Rapid7 ha hecho pública una vulnerabilidad que afecta al firewall Zyxel y sus dispositivos VPN para empresas, y que podría permitir a un atacante remoto inyectar comandos arbitrarios sin autenticación, habilitando de esta forma la configuración de una shell inversa.

Los productos afectados son muy comunes tanto en implementaciones de oficinas pequeñas como en sucursales centrales corporativas. Entre sus servicios destacan la prestación de soluciones VPN, la inspección SSL, el filtrado web, la protección contra intrusiones y la seguridad para el correo electrónico. Los modelos vulnerables son relativamente populares, con más de 15.000 dispositivos potencialmente vulnerables desplegados en varios países, según se indica en Shodan.

La vulnerabilidad, rastreada como CVE-2022-30525, fue descubierta por el investigador Jacob Baines, y permite a un atacante establecer una shell inversa utilizando el bash GTFOBin normal. De manera adicional, otros investigadores se han sumado al estudio de esta vulnerabilidad, en concreto, destaca la organización sin ánimo de lucro Shadowserver, quienes observaron indicios de que el fallo estaba siendo explotado. Por su parte, el analista z3r00t creó y publicó una plantilla que permite a los usuarios realizar un escaneo de vulnerabilidades y comprobar si los dispositivos son vulnerables. Además, el investigador BlueNinja, publicó un script para detectar la inyección de comandos remotos no autenticados en los productos VPN y cortafuegos de Zyxel. para detectar la inyección de comandos remotos no autenticados en los productos VPN y cortafuegos de Zyxel.


Imagen 1: Tweet del investigador Jacob Baine alertando de la vulnerabilidad

## 2. ANÁLISIS TÉCNICO

La vulnerabilidad, descubierta por el principal investigador de seguridad de Rapid7, Jacob Baines, y rastreada bajo el CVE-2022-30525, permite que un atacante ejecute comandos arbitrarios de forma remota sin autenticación, lo que puede llegar a provocar, entre otras acciones, que se habilite la configuración de una shell inversa.

A continuación, se muestra una lista con los modelos afectados por esta vulnerabilidad:

- USG FLEX 100 (An), 200, 500, 700. ZLD V5.00 a ZLD V5.21 parche 1.
- USG FLEX 50(W) / USG20(W)-VPN. ZLD V5.10 a ZLD V5.21 parche 1.
- Serie ATP. ZLD V5.10 a ZLD V5.21 Parche 1.
- Serie VPN. ZLD V4.60 a ZLD V5.21 Parche 1.

Los modelos indicados anteriormente son vulnerables a la inyección de comandos de forma remota a través de la interfaz HTTP administrativa. Los comandos se ejecutan como *nobody user,* nombre convencional de un identificador de usuario que no posee ningún archivo, no está en ningún grupo privilegiado y no tiene ninguna capacidad excepto las que tiene cualquier otro usuario. Normalmente no está habilitado como cuenta de usuario, es decir, no tiene asignado ningún directorio root ni credenciales de acceso.

Esta vulnerabilidad se explota a través de la ruta */ztp/cgi-bin/handle,* y es el resultado de pasar la entrada del atacante sin desinfectar a la función *os.system* en el archivo *lib_wan_settings.py*. La funcionalidad vulnerable se explota en asociación con el comando *setWanPortSt*. Un atacante, de forma remota, puede inyectar comandos arbitrarios en los parámetros de dicha función.

Esta vulnerabilidad, a la cual se le ha otorgado un impacto crítico debido al gran despliegue de los dispositivos vulnerables en numerosas compañías de todo el mundo, está siendo explotada activamente desde el pasado 13 de mayo, según han asegurado expertos en ciberseguridad de la organización sin fines de lucro Shadowserver. No obstante, todavía no se ha confirmado si estas actividades detectadas son maliciosas o solo investigaciones que trabajan para mapear dispositivos Zyxel actualmente expuestos a ataques.

Se ha desarrollado un módulo de Metasploit para esta vulnerabilidad, el cual se puede utilizar para establecer una sesión de *nobody user* de Meterpreter. En el siguiente enlace se dispone de un video explicativo:

- Zyxel Firewall Unauthenticated Command Inject (CVE-2022-30525) Metasploit Module.

## 3. MITIGACIÓN / SOLUCIÓN

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

Zyxel ha lanzado los parches correspondientes para abordar esta vulnerabilidad e insta a los usuarios a instalarlos para obtener una protección completa. A continuación, se presenta en una tabla los modelos y las versiones afectadas en relación con el parche disponible para su mitigación.

| Modelo afectado | Versión firmware afectada | Parche disponible |
|---|---|---|
| USG FLEX 100(W), 200, 500, 700 | ZLD V5.00 - V5.21 | ZLD V5.30 |
| USG FLEX 50(W) / USG20(W)-VPN | ZLD V5.10- V5.21 | ZLD V5.30 |
| ATP series | ZLD V5.10- V5.21 | ZLD V5.30 |
| VPN series | ZLD V4.60 - V5.21 | ZLD V5.30 |

Además, desde el fabricante, se recomienda, en la medida de lo posible, mantener activadas las actualizaciones automáticas del firmware y deshabilitar el acceso WAN a la interfaz web administrativa del sistema.

Por último, destacar la publicación de una regla suricata que captura la explotación de esta vulnerabilidad. Esta regla se ha probado utilizando el módulo Metasploit indicado en el apartado.

```
alert http any any -> any any ( \
   msg:"Possible Zyxel ZTP setWanPortSt mtu Exploit Attempt"; \
   flow:to_server; \
   http.method; content:"POST"; \
   http.uri; content:"/ztp/cgi-bin/handler"; \
   http.request_body; content:"setWanPortSt"; \
   http.request_body; content:"mtu"; \
   http.request_body; pcre:"/mtu['"]\s*:\s*['"]\s*[^0-9]+/i";
   classtype:misc-attack; \
   sid:221270;)
```

Imagen 2: Regla suricata publicada para la detección de la vulnerablidad.

# 4. REFERENCIAS ADICIONALES


- CVE-2022-30525 (FIXED): Zyxel Firewall Unauthenticated Remote Command Injection.
- Zyxel security advisory for OS command injection vulnerability of firewalls.
- Hackers are exploiting critical bug in Zyxel firewalls and VPNs.
- Critical flaw in Zyxel firewalls grants access to corporate networks (CVE-2022-30525).
- Zyxel Firewall Unauthenticated Command Inject (CVE-2022-30525) Metasploit Module.
- Github: Zyxel Firewall Unauthenticated Command Injection (CVE-2022-30525).
- Github: CVE-2022-30525-initial-detect.yaml.
- Github: cve-2022-30525.yaml.
- Gtfobins: reverse-shell.
- Rapid7 official page.
- Zyxel Networks official page.
- Shadowserver Foundation official twitter page.
- z3r00t official twitter page.
- __blueNinja official twitter page.
- Shodan: Implementación dispositivos Zyxel.
- NIST: CVE-2022-30525.
- Reverse shell, una curiosa y al mismo tiempo peligrosa técnica.


## Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

## Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?