Basque CyberSecurity Centre

# Vulnerabilidades explotadas para implementar el malware Zerobot

**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 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

El equipo de investigación de Microsoft (MSTIC), ha publicado un estudio sobre la actualización de Zerobot, una red de bots ofrecida como *malware-as-a-service*, basada en Go y que aprovecha distintas vulnerabilidades que afectan a aplicaciones web e IoT.

Tras un análisis de la última versión utilizada de Zerobot, los investigadores han logrado detectar la suma de exploits a su lista de vulnerabilidades, pudiendo identificar un total de siete errores destacados por tener una severidad alta o crítica, entre los que se encuentran 2 vulnerabilidades que afectan a sistemas Apache HTTP Server y Apache Spark.

La finalidad de añadir nuevas vulnerabilidades que explotar en sus campañas, radica en la intención existente por parte de los actores de amenazas de llevar a cabo un aumento en la infección de dispositivos firewall, routers y demás sistemas vulnerables, para ser añadidos a su red de bots de denegación de servicio distribuido (DDoS).

Algunos de los fabricantes de los sistemas vulnerables ya han publicado los parches correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas 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.

## 2. Análisis técnico

Las vulnerabilidades incluidas por la versión 1.1 de Zerobot, salvo una de ellas con una criticidad alta, han sido calificadas con una severidad crítica por parte del NIST.

Primeramente, se detalla la vulnerabilidad identificada bajo el CVE-2017-17105, cuya severidad es crítica, asignándole una puntuación de 9.8 según la escala CVSSv3. Dicho fallo, reportado inicialmente por parte del investigador Silas Cutler, permite a un atacante remoto no autenticado inyectar código arbitrario mediante scripts *CGI*. Este error afecta a distintas versiones de las cámaras web Zivif PR115-204-P-RS. Cabe destacar que se ha detectado la disponibilidad de manera pública de una prueba de concepto (PoC) para explotar el fallo descrito.

Seguidamente, se destaca la vulnerabilidad catalogada bajo el CVE-2019-10655, cuya severidad es crítica, contando con una puntuación de 9.8 en relación a la escala CVSSv3. Esta vulnerabilidad permite a un atacante remoto no autenticado, ejecutar código arbitrario en el sistema destino mediante *metacaracteres de shell*, dando lugar de esta manera a un desbordamiento de búfer. Un actor de amenazas podrá sobrescribir una estructura de datos maliciosa, eludiendo así la autenticación del sistema. Esta vulnerabilidad, que afecta a dispositivos Grandstream GAC2500, GXP2200, GVC3202 y GXV3275, puede ser explotada de manera remota o vía *Cross-Site Request Forgery* (CSRF). Asimismo, se ha identificado un módulo de Metasploit de acceso público que contiene una prueba de concepto (PoC) para explotar el fallo descrito.

La tercera vulnerabilidad destacada está identificada bajo el CVE-2020-25223, teniendo una severidad crítica, contando con una puntuación de 9.8 en relación a la escala CVSSv3. Se conoce que dicha vulnerabilidad permite a un atacante remoto ejecutar código arbitrario de manera remota en distintas versiones de Sophos SG UTM. Adicionalmente, se ha detectado la publicación de un módulo de Metasploit que contiene una prueba de concepto (PoC) para explotar el fallo descrito.

El cuarto error detectado, que se encuentra registrado bajo el CVE-2021-42013 cuenta con una severidad crítica, teniendo asignada una puntuación de 9.8 de acuerdo a la escala CVSSv3. La vulnerabilidad a un atacante remoto no autenticado, enviar una solicitud HTTP especialmente diseñada al servidor afectado y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino. El error, que afecta a distintas versiones de los servidores Apache, cuenta con diversas pruebas de concepto (PoC), accesibles a través de los siguientes enlaces:

- Apache HTTP Server 2.4.50 Path Traversal / Code Execution.
- Apache 2.4.49 / 2.4.50 Traversal / Remote Code Execution.
- Apache HTTP Server 2.4.50 Remote Code Execution.
- Apache 2.4.50 Remote Code Execution.

Seguidamente, encontramos la vulnerabilidad registrada bajo el CVE-2022-31137, que cuenta con una severidad crítica, teniendo una puntuación de 9.8 sobre la escala CVSSv3. La vulnerabilidad existe debido a una validación de entrada inadecuada pasada a través de la función *subprocess_execute()* al archivo */app/options.py*. Un atacante remoto no autenticado puede pasar una solicitud HTTP especialmente diseñada y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino. Cabe destacar que dicho fallo, que afecta a la interfaz web Roxi-WI, cuenta con un exploit que se puede consultar públicamente.

La sexta vulnerabilidad, identificada bajo el CVE-2022-33891, tiene una severidad alta con una puntuación de 8.8 de acuerdo a la escala CVSSv3. La vulnerabilidad existe debido a una validación de entrada inadecuada en la función *ACL* dentro de la interfaz de usuario de Apache Spark. Un usuario remoto puede solicitar una URL especialmente diseñada y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable, pero requiere que la opción *spark.acls.enable* esté activada. Cabe destacar que se ha detectado un módulo de Metasploit de manera pública que detalla una prueba de concepto (PoC) en relación a la vulnerabilidad descrita.

Por último, la vulnerabilidad reportada por el investigador Gjoko Krstic y catalogada bajo el ZLS-2022-5717, ha sido puntuada con una severidad crítica. Se tiene el conocimiento de que este fallo permite a un atacante remoto no autenticado ejecutar código arbitrario con privilegios de *root*. En el aviso publicado, se encuentra un enlace que redirige a una prueba de concepto (PoC) que proporciona los detalles para aprovechar el error que afecta a MiniDVBLinux.

Los productos afectados por las anteriores vulnerabilidades son los siguientes:

- Zivif PR115-204-P-RS versiones 2.3.4.2103 – 4.7.4.2121.
- Granstream GAC2500 versión 1.0.3.35.
- Granstream GXP2200 versión 1.0.3.51.
- Granstream GXV3275 versiones anteriores a 1.0.3.219 Beta.

- Granstream GXV3240 versiones anteriores a 1.0.3.219 Beta.
- Sophos SG UTM versiones anteriores a v9.705 MR5, v9.607 MR7 y v9.511 MR11.
- Apache HTTP Server version 2.4.50.
- Roxi-WI versiones anteriores a 6.1.1.0.
- Apache Spark versiones 3.03 y anteriores, 3.1.1 – 3.1.2 y 3.2.0 – 3.2.1.
- MiniDVBLinux versión 5.4 y anteriores.

## 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.

Es importante que se tomen medidas rápidamente para mitigar estos problemas en la implementación. Por ello, dada la gravedad de las vulnerabilidades, se recomienda aplicar las soluciones oficiales propuestas por los fabricantes, disponibles en los siguientes enlaces:

- Grandstream GAC2500 versión 1.0.3.45.
- Grandstream GVC3202 versión 1.0.3.69.
- Grandstream GXV3275 versión 1.0.3.227.
- Grandstream GXV3240 versión 1.0.3.227.
- Apache HTTP Server versión 2.4.54.
- Roxi-WI versión 6.1.1.0.
- Apache Spark versión 3.3.1.
- MiniDVBLinux versión 5.5.

Cabe destacar que actualmente no se tiene conocimiento de que exista una solución oficial para el CVE-2017-17105. En relación al CVE-2019-10655, el proveedor no ha publicado una mitigación que solucione dicho error en Granstream GXP2200.

Finalmente, la versión 5.5 de MiniDVBLinux no es estable, pero se recomienda su instalación ya que mitiga la vulnerabilidad crítica y registrada bajo ZLS-2022-5717.

## 4. Referencias Adicionales


- MSTIC.
- Microsoft research uncovers new Zerobot capabilities.
- Apache HTTP Server.
- Apache Spark.
- NIST.
- NVD: CVE-2017-17105.
- NVD: CVE-2019-10655.
- NVD: CVE-2020-25223.
- NVD: CVE-2021-42013.
- NVD: CVE-2022-31137.
- NVD: CVE-2022-33891.
- ZLS-2022-5717.
- First organization.
- Contenido dinámico con CGI.
- Zivif PR115-204-P-RS 2.3.4.2103 Bypass / Command Injection / Hardcoded Password.
- Comandos en Linux: metacaracteres, entrecomillado y caracteres especiales.
- ¿En qué consiste la vulnerabilidad Cross Site Request Forgery (CSRF)?
- Grandstream GXV3175 Unauthenticated Command Execution.
- Sophos UTM WebAdmin SID Command Injection.
- Apache HTTP Server 2.4.50 Path Traversal / Code Execution.
- Apache 2.4.49 / 2.4.50 Traversal / Remote Code Execution.
- Apache HTTP Server 2.4.50 Remote Code Execution.
- Apache 2.4.50 Remote Code Execution.
- Roxy-WI Remote Command Execution.
- Lista de control de acceso (ACL) en la red.
- ACL Configuration for Spark.

- Apache Spark Unauthenticated Command Injection.
- PoC: ZLS-2022-5717.
- Grandstream GAC2500 versión 1.0.3.45.
- Grandstream GVC3202 versión 1.0.3.69.
- Grandstream GXV3275 versión 1.0.3.227.
- Grandstream GXV3240 versión 1.0.3.227.
- Apache HTTP Server versión 2.4.54.
- Roxi-WI versión 6.1.1.0.
- Apache Spark versión 3.3.1.
- MiniDVBLinux versión 5.5.
- Grandstream Important Firmware News.


EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA