Basque CyberSecurity Centre

Vulnerabilidad en FortiOS (CVE-2022-42475)

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

Fortinet ha publicado una actualización de seguridad en la que se trata una vulnerabilidad de severidad crítica y CVSS 9.3, de desbordamiento de búfer basado en el heap en FortiOS, cuyo identificador es CVE-2022-42475.

Por otra parte, como refleja la nota de seguridad ofrecida por la compañía, el fallo está siendo **explotado**.

2. Recursos afectados

- Versiones de FortiOS: 7.2.2, 7.2.1, 7.2.0, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.9, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.10, 6.4.1, 6.4.0, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.11, 6.2.10, 6.2.1, 6.2.0

3. Análisis técnico

La vulnerabilidad identificada como CVE-2022-42475 se corresponde con un desbordamiento de búfer basado en el heap en FortiOS SSL-VPN, de manera que un atacante remoto no autenticado puede ejecutar código o comandos arbitrarios a través de solicitudes diseñadas específicamente, pudiéndose aprovechar este fallo para tomar el control de un sistema no actualizado.

La métrica de la vulnerabilidad se corresponde de:

CVSS Base: 9.3, crítica

CWE-122: Desbordamiento de búfer basado en el heap

4. Mitigación / Solución

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

Por ello, dada la criticidad de este fallo, Fortinet recomienda a sus clientes aplicar la actualización proporcionada por la compañía y a verificar los siguientes indicadores de compromiso:

- Múltiples entradas de registro (logs) con:

  Logdesc="Application crashed" and msg="[...] application:sslvpnd,[...], Signal 11 received, Backtrace: [...]“

- Presencia de los siguientes artefactos en el sistema de archivos:

  /data/lib/libips.bak
  /data/lib/libgif.so
  /data/lib/libiptcp.so
  /data/lib/libipudp.so
  /data/lib/libjepg.so
  /var/.sslvpnconfigbk
  /data/etc/wxd.conf
  /flash

- Conexiones a direcciones IP sospechosas desde FortiGate:

  188.34.130.40:444

  103.131.189.143:30080,30081,30443,20443

  192.36.119.61:8443,444

  172.247.168.153:8033

5. Referencias Adicionales

- CVE-2022-42475
- Nota de seguridad de Fortinet
- FortiOS
- CWE-122


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA