Basque CyberSecurity Centre

Vulnerabilidades en FortiADC y FortiTester (CVE-2022-39947, CVE-2022-35845)

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 dos notas de seguridad que afectan a los productos FortiADC y FortiTester. Las vulnerabilidades tratadas, CVE-2022-39947 y CVE-2022-35845, cuentan con una severidad alta y pueden producir una inyección de comandos no autorizados, tanto en la interfaz web de FortiADC como en la GUI y la API de FortiTester respectivamente.

2. Recursos afectados

- FortiADC versiones: 7.0.2, 7.0.1, 7.0.0, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.1.6, 6.1.5, 6.1.4, 6.1.3, 6.1.2, 6.1.1, 6.1.0, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0, 5.4.5, 5.4.4, 5.4.3, 5.4.2, 5.4.1, 5.4.0
- FortiTester versiones: 7.1.0, 7.0.0, 4.2.0, 4.1.1, 4.1.0, 4.0.0, 3.9.1, 3.9.0, 3.8.0, 3.7.1, 3.7.0, 3.6.0, 3.5.1, 3.5.0, 3.4.0, 3.3.1, 3.3.0, 3.2.0, 3.1.0, 3.0.0, 2.9.0, 2.8.0, 2.7.0, 2.6.0, 2.5.0, 2.4.1, 2.4.0, 2.3.0

3. Análisis técnico

La vulnerabilidad, identificada como CVE-2022-39947, se corresponde con una neutralización incorrecta de elementos especiales utilizados en un comando OS (inyección de comandos del sistema operativo) en Fortinet FortiADC que puede permitir a un atacante ejecutar código o comandos no autorizados a través de solicitudes HTTP específicamente diseñadas.

La métrica de evaluación de la vulnerabilidad es la siguiente:

CVSS Base: 8.8, alta

CWE 78: neutralización incorrecta de elementos especiales utilizados en un comando del sistema operativo (inyección de comandos del sistema operativo)

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

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

En cuanto a la vulnerabilidad CVE-2022-35845, es debida a la neutralización incorrecta múltiple de elementos especiales utilizados en un comando del sistema operativo (inyección de comandos del sistema operativo) en FortiTester puede permitir que un atacante autenticado ejecute comandos arbitrarios en el shell subyacente.

La métrica de evaluación de la vulnerabilidad es la siguiente:

CVSS Base: 7.8, alta

CWE 78: neutralización incorrecta de elementos especiales utilizados en un comando del sistema operativo (Inyección de comandos del sistema operativo)

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

- **Vector de ataque**: Local
- **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, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para solucionar estos fallos, desde Fortinet se recomienda en el caso de FortiADC:

- Actualizar a la versión FortiADC 7.0.2
- Actualizar a la versión FortiADC 6.2.4

En cuanto a FortiTester, Fortinet recomienda:

- Actualizar a FortiTester versión 7.2.0 o superior
- Actualizar a FortiTester versión 7.1.1 o superior
- Actualizar a FortiTester versión 4.2.1 o superior
- Actualizar a FortiTester versión 3.9.2 o superior

5. Referencias Adicionales

- Notas de seguridad de Fortinet
- CVE-2022-39947
- CVE-2022-35845
- FortiADC
- FortiTester
- CWE 78

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA