Vulnerabilidades críticas en FortiOS y FortiClientEMS

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca. 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.

1. Resumen ejecutivo

Fortinet ha publicado varios avisos de seguridad para tratar **3 vulnerabilidades de severidad crítica**, cuyos identificadores son CVE-2023-42789, CVE-2023-42790 y CVE-2023-48788, las cuales afectan al **producto FortiOS,** y **3 vulnerabilidades de severidad alta,** cuyos identificadores son CVE-2023-47534, CVE-2024-23112 y CVE-2023-36554, las cuales afectan al producto **FortiClientEMS**.

Estas vulnerabilidades suponen una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas que se puedan ver afectados.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

- FortiClientEMS 7.2 de la versión 7.2.0 hasta la 7.2.2.
- FortiClientEMS 7.0 de la version 7.0.0 hasta la 7.0.10.
- FortiClientEMS 6.4 todas las versiones.
- FortiClientEMS 6.2 todas las versiones.
- FortiClientEMS 6.0 todas las versiones.
- FortiOS de la verión 7.4.0 hasta la 7.4.1.
- FortiOS de la version 7.2.0 hasta la 7.2.5.
- FortiOS de la versión 7.0.0 hasta la 7.0.12.
- FortiOS de la versión 6.4.0 hasta la 6.4.14.
- FortiOS de la version 6.2.0 hasta la 6.2.15.
- FortiProxy version 7.4.0.
- FortiProxy de la version 7.2.0 hasta la 7.2.6.
- FortiProxy de la version 7.0.0 hasta la 7.0.12.
- FortiProxy de la versión 2.0.0 hasta la 2.0.13.
- FortiOS 7.2 de la versión 7.2.0 hasta la 7.2.6.
- FortiOS 7.0 de la versión 7.0.1 hasta la 7.0.13.
- FortiOS 6.4 de la versión 6.4.7 hasta la 6.4.14.
- FortiProxy 7.4 de la versión 7.4.0 hasta la 7.4.2.
- FortiProxy 7.2 de la versión 7.2.0 hasta la 7.2.8.
- FortiProxy 7.0 de la versión 7.0.0 hasta la 7.0.14.
- FortiManager versión 7.4.0.
- FortiManager versión 7.2.0 hasta la 7.2.3.
- FortiManager versión 7.0.0 hasta la 7.0.10.
- FortiManager versión 6.4.0 hasta la 6.4.13.
- FortiManager 6.2 todas las versiones.

3. Análisis técnico

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

CVE-2023-42789: vulnerabilidad de escritura fuera de límites que afecta a **Fortinet FortiOS** y **Fortinet FortyProxy** en las siguientes versiones:

- FortiOS 7.4.0 hasta la versión 7.4.1.
- FortiOS 7.2.0 hasta la versión 7.2.5.
- FortiOS 7.0.0 hasta la versión 7.0.12.
- FortiOS 6.4.0 hasta la versión 6.4.14.
- FortiOS 6.2.0 hasta la versión 6.2.15.
- FortiProxy 7.4.0.
- FortiProxy 7.2.0 hasta la versión 7.2.6.
- FortiProxy 7.0.0 hasta la versión 7.0.12.
- FortiProxy 2.0.0 hasta la versión 2.0.13.

La explotación de esta vulnerabilidad permite a un atacante ejecutar código o comandos no autorizados a través de solicitudes HTTP especialmente diseñadas.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-787: Out-of-bounds Write

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: Ninguno**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-42790: vulnerabilidad de desbordamiento de búfer basado en pila en el portal cautivo de **FortiOS** y **FortiProxy** pueden permitir a un atacante interno acceder a dicho portal y ejecutar código o comandos arbitrarios a través de solicitudes HTTP especialmente diseñadas.

Las versiones de **FortiOS** y **FortiProxy** afectadas son las siguientes:

- FortiOS 7.4.0 hasta la versión 7.4.1.
- FortiOS 7.2.0 hasta la versión 7.2.5.
- FortiOS 7.0.0 hasta la versión 7.0.12.
- FortiOS 6.4.0 hasta la versión 6.4.14.
- FortiOS 6.2.0 hasta la versión 6.2.15.

- FortiProxy 7.4.0.
- FortiProxy 7.2.0 hasta la versión 7.2.6.
- FortiProxy 7.0.0 hasta la versión 7.0.12.
- FortiProxy 2.0.0 hasta la versión 2.0.13.

La métrica de evaluación de esta vulnerabilidad se compone de:

CWE-121: Stack-based Buffer Overflow

CVSS Base: **8.1**

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: Ninguno**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-48788: vulnerabilidad de neutralización inadecuada de elementos especiales utilizados en un comando SQL (SQL Injection) en FortiClientEMS puede permitir a un atacante no autenticado ejecutar código no autorizado o comandos a través de peticiones específicamente elaboradas.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL 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: Ninguno**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-47534: vulnerabilidad causada por una neutralización inapropiada de elementos de fórmula en un archivo CSV en Fortinet FortiClientEMS. La explotación de esta vulnerabilidad permitiría a un atacante ejecutar código o comandos no autorizados a través de paquetes especialmente diseñados.

Las versiones de FortiClientEMS afectadas son las siguientes:

- FortiClientEMS desde la versión 7.2.0 hasta la versión 7.2.2.
- FortiClientEMS desde la versión 7.0.0 hasta la versión 7.0.10.
- FortiClientEMS desde la versión 6.4.0 hasta la versión 6.4.9.
- FortiClientEMS desde la versión 6.2.0 hasta la versión 6.2.9.
- FortiClientEMS desde la versión 6.0.0 hasta la versión 6.0.8.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-1236: Improper Neutralization of Formula Elements in a CSV File

CVSS Base: **9.6**

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario**: Requerida
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-23112: vulnerabilidad causada por la omisión de autorización a través de la clave controlada por el usuario en FortiOS y FortiProxy SSLVPN puede permitir a un atacante autenticado obtener acceso al marcador de otro usuario a través de la manipulación de URL.

Las versiones de FortiOS y FortiProxy afectadas son las siguientes:

- FortiOS desde la versión 7.4.0 hasta la versión7.4.1.
- FortiOS desde la versión versión7.2.0 hasta la versión 7.2.6.
- FortiOS desde la versión 7.0.1 hasta la versión 7.0.13.
- FortiOS desde la versión 6.4.7 hasta la versión 6.4.14.
- FortiProxy desde la versión 7.4.0 hasta la versión 7.4.2.
- FortiProxy desde la versión 7.2.0 hasta la versión 7.2.8.
- FortiProxy desde la versión 7.0.0 hasta la versión 7.0.14.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-639: Authorization Bypass Through User-Controlled Key

CVSS Base: **8.0**

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

- **Vector de ataque:** Adyacente
- **Complejidad del ataque:** Alta

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

CVE-2023-36554: vulnerabilidad de control de acceso incorrecto en FortiWLM MEA para FortiManager puede permitir a un atacante remoto no autenticado ejecutar código o comandos arbitrarios a través de solicitudes específicamente diseñadas.

Las versiones de FortiManager afectadas son las siguientes:

- FortiManager versión 7.4.0
- FortiManager desde la versión 7.2.0 hasta la versión 7.2.3.
- FortiManager desde la versión 7.0.0 hasta la versión 7.0.10.
- FortiManager desde la versión 6.4.0 hasta la versión 6.4.13.
- FortiManager 6.2 todas las versiones.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-284: Improper Access Control

CVSS Base: **8.1**

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

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

4. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para corregir las vulnerabilidades CVE-2023-42789 y CVE-2023-42790, Fortinet recomienda:

- Actualizar a FortiOS 7.4.0 o superior
- Actualizar a FortiOS 7.4.2 o superior
- Actualizar a FortiOS 7.2.6 o superior
- Actualizar a FortiOS 7.0.13 o superior
- Actualizar a FortiOS 6.4.15 o superior
- Actualizar a FortiOS 6.2.16 o superior
- Actualizar a FortiProxy 7.4.1 o superior
- Actualizar a FortiProxy 7.2.7 o superior
- Actualizar a FortiProxy 7.0.13 o superior
- Actualizar a FortiProxy 2.0.14 o superior

Para corregir la vulnerabilidad CVE-2023-48788 Fortinet recomienda:

- Actualizar a FortiClientEMS 7.2.3 o superior
- Actualizar a FortiClientEMS 7.0.11 o superior

Para corregir la vulnerabilidad CVE-2023-47534 Fortinet recomienda:

- Actualizar FortiClientEMS 7.2 a 7.2.3 o superior
- Actualizar FortiClientEMS 7.0 a 7.0.11 o superior
- Migrar FortiClientEMS 6.4 a una versión corregida
- Migrar FortiClientEMS 6.2 a una versión corregida
- Migrar FortiClientEMS 6.0 a una versión corregida

Para corregir la vulnerabilidad CVE-2024-23112 Fortinet recomienda:

- Actualizar FortiOS 7.4 a 7.4.2 o superior
- Actualizar FortiOS 7.2 a 7.2.7 o superior
- Actualizar FortiOS 7.0 a 7.0.14 o superior
- Actualizar FortiOS 6.4 a 6.4.15 o superior
- Actualizar FortiProxy 7.4 a 7.4.3 o superior
- Actualizar FortiProxy 7.2 a 7.2.9 o superior
- Actualizar FortiProxy 7.0 a 7.0.15 o superior

Para corregir la vulnerabilidad CVE-2023-36554 Fortinet recomienda:

- FortiManager actualizar a la versión 7.4.1 o superior
- FortiManager actualizar a la versión 7.2.4 o superior
- FortiManager actualizar a la versión 7.0.11 o superior
- FortiManager actualizar a la versión 6.4.14 o superior

5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2023-42789.
- CVE-2023-42790.
- CVE-2023-48788.
- CVE-2023-47534.
- CVE-2024-23112.
- CVE-2023-36554.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY