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 **2 vulnerabilidades de severidad critica**, cuyos identificadores son CVE-2024-23113 y CVE-2024-21762, que afectan al **producto FortiOS** y **1 vulnerabilidad de severidad alta** cuyo identificador es CVE-2023-45581, que afecta 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

- FortiOS 6.0 todas las versiones.
- FortiOS 6.2 de la version 6.2.0 a la version 6.2.15.
- FortiOS 6.4 de la version 6.4.0 a la version 6.4.14.
- FortiOS 7.0 de la version 7.0.0 a la version 7.0.13.
- FortiOS 7.2 de la version 7.2.0 a la version 7.2.6.
- FortiOS 7.4 de la version 7.4.0 a la version 7.4.2.
- FortiClientEMS 6.2 todas las versiones.
- FortiClientEMS 6.4 todas las versiones.
- FortiClientEMS 7.0 de la version 7.0.0 a la version 7.0.4.
- FortiClientEMS 7.0 de la version 7.0.6 a la version 7.0.10.
- FortiClientEMS 7.2 de la version 7.2.0 a la version 7.2.2.

3. Análisis técnico

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

CVE-2024-23113: vulnerabilidad de cadena de formato controlada externamente en el demonio fgfmd de FortiOS que podría permitir a un atacante remoto no autenticado ejecutar código o comandos arbitrarios mediante solicitudes especialmente diseñadas.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 134: Use of Externally-Controlled Format String

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-2024-21762: vulnerabilidad de escritura fuera de límites en FortiOS que podría permitir a un atacante remoto no autenticado ejecutar código o comandos arbitrarios mediante solicitudes HTTP especialmente diseñadas.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 787: Out-of-bounds Write

CVSS Base: **9.6**

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-2023-45581: vulnerabilidad de gestión de privilegios inadecuada en la interfaz administrativa gráfica de FortiClientEMS que podría permitir a un administrador del sitio con privilegios de Super Administrador realizar

operaciones administrativas globales que afecten a otros sitios a través de solicitudes HTTP o HTTPS manipuladas.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 269: Improper Privilege Management

CVSS Base: **7.9**

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**

4. Mitigación / Solución

Como es habitual, para prevenir esta 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 la vulnerabilidad CVE-2024-23113 Fortinet recomienda:

- Actualizar FortiOS 7.0 a la versión 7.0.14 o superior.
- Actualizar FortiOS 7.2 a la versión 7.2.7 o superior.
- Actualizar FortiOS 7.4 a la versión 7.4.3 o superior.

Para corregir la vulnerabilidad CVE-2024-21762 Fortinet recomienda:

- Migrar FortiOS 6.0 a una versión corregida.
- Actualizar FortiOS 6.2 a la versión 6.2.16 o superior
- Actualizar FortiOS 6.4 a la versión 6.4.15 o superior.
- Actualizar FortiOS 7.0 a la versión 7.0.14 o superior.
- Actualizar FortiOS 7.2 a la versión 7.2.7 o superior.
- Actualizar FortiOS 7.4 a la versión 7.4.3 o superior.

Para corregir la vulnerabilidad CVE-2023-45581 Fortinet recomienda:

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

5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2024-21762
- CVE-2024-23113
- CVE-2023-45581


cyber
zaintza
BASQUE CYBERSECURITY AGENCY