Vulnerabilidades en FortiOS, FortiClientLinux, FortiProxy y FortiSandBox

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

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 **1 vulnerabilidad de severidad crítica**, cuyo identificador es CVE-2023-45590, que afecta al **producto FortiClientLinux,** y **6 vulnerabilidades de severidad alta,** cuyos identificadores son CVE-2023-45588, CVE-2024-31492, CVE-2023-41677, CVE-2024-23671, CVE-2024-21755 y CVE-2024-21756 que afectan a los productos **FortiClientMac installer**, **FortiProxy** y **FortiSandbox**.

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

- FortiClientLinux 7.2 afecta a la versión 7.2.0.
- FortiClientLinux 7.0 desde la versión 7.0.6 hasta la version 7.0.10.
- FortiClientLinux 7.0 desde la versión 7.0.3 hasta la version 7.0.4.
- FortiClientMac 7.2 de la versión 7.2.0 hasta la 7.2.3.
- FortiClientMac 7.0 de la version 7.0.6 hasta la 7.0.10.
- FortiOS 7.4 desde la versión 7.4.0 hasta la versión 7.4.1.
- FortiOS 7.2 desde la versión 7.2.0 hasta la versión 7.2.6.
- FortiOS 7.0 desde la versión 7.0.0 hasta la versión 7.0.12.
- FortiOS 6.4 desde la versión 6.4.0 hasta la versión 6.4.14.
- FortiOS 6.2 desde la versión 6.2.0 hasta la versión 6.2.15.
- FortiOS 6.0 desde la versión 6.0 todas las versiones.
- FortiProxy 7.4 desde la versión 7.4.0 hasta la versión 7.4.1.
- FortiProxy 7.2 desde la versión 7.2.0 hasta la versión 7.2.7.
- FortiProxy 7.0 desde la versión 7.0.0 hasta la versión 7.0.13.
- FortiProxy 2.0 desde la versión 2.0 todas las versiones.
- FortiProxy 1.2 desde la versión 1.2 todas las versiones.
- FortiProxy 1.1 desde la versión 1.1 todas las versiones.
- FortiProxy 1.0 desde la versión 1.0 todas las versiones.
- FortiSandbox 4.4 desde la versión 4.4.0 hasta la versión 4.4.3.
- FortiSandbox 4.2 desde la versión 4.2.0 hasta la versión 4.2.6.
- FortiSandbox 4.0 desde la versión 4.0.0 hasta la versión 4.0.4.

3. Análisis técnico

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

CVE-2023-45590: vulnerabilidad de severidad crítica de control inadecuado de generación de código (inyección de código) que afecta a FortiClientLinux. La explotación de esta vulnerabilidad podría permitir a un atacante no autenticado ejecutar código arbitrario al engañar a un usuario de FortiClientLinux para que visite un sitio web malicioso.

Las versiones de FortiClient Linux afectadas por esta vulnerabilidad son las siguientes:

- FortiClientLinux 7.2 afecta a la versión 7.2.0.
- FortiClientLinux 7.0 desde la versión 7.0.6 hasta la versión 7.0.10.
- FortiClientLinux 7.0 desde la versión 7.0.3 hasta la versión 7.0.4.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-94: Improper Control of Generation of Code (Code Injection)

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-2024-21755, CVE-2024-21756: vulnerabilidades de neutralización inadecuada de elementos especiales utilizados en comandos del sistema operativo en FortiSandbox pueden permitir que un atacante autenticado con al menos permisos de solo lectura ejecute comandos no autorizados a través de solicitudes manipuladas.

Las versiones de FortiSandbox afectadas son las siguientes:

- FortiSandbox 4.4 desde la versión 4.4.0 hasta la versión 4.4.3.
- FortiSandbox 4.2 desde la versión 4.2.0 hasta la versión 4.2.6.
- FortiSandbox 4.0 desde la versión 4.0.0 hasta la versión 4.0.4.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CVSS Base: **8.8**

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

CVE-2024-23671: vulnerabilidad de limitación inadecuada de una ruta de acceso a un directorio restringido que afecta a FortiSandbox. La explotación de esta vulnerabilidad puede permitir que un atacante autenticado con al menos permisos de solo lectura elimine archivos arbitrarios mediante solicitudes HTTP manipuladas.

Las versiones de FortiSandbox afectadas son las siguientes:

- FortiSandbox 4.4 desde la versión 4.4.0 hasta la versión 4.4.3.
- FortiSandbox 4.2 desde la versión 4.2.0 hasta la versión 4.2.6.
- FortiSandbox 4.0 desde la versión 4.0.0 hasta la versión 4.0.4.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-22: Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)

CVSS Base: **8.1**

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**

CVE-2023-45588, CVE-2024-31492: vulnerabilidades de control externo de nombre de archivo o ruta en el instalador de FortiClientMac, que podrían permitir, que un atacante local, ejecute código o comandos arbitrarios al escribir un archivo de configuración malicioso en /tmp antes de iniciar el proceso de instalación.

Las versiones de **FortClientMac** afectadas son las siguientes:

- FortiClientMac 7.2 de la versión 7.2.0 hasta la 7.2.3.
- FortiClientMac 7.0 de la version 7.0.6 hasta la 7.0.10.

La métrica de evaluación de esta vulnerabilidad se compone de:

CWE-73: External Control of File Name or Path

CVSS Base: **7.8**

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

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

CVE-2023-41677: vulnerabilidad de credenciales insuficientemente protegidas en FortiOS y FortiProxy, cuya explotación podría permitir a un atacante la obtención de la cookie del administrador al engañar al administrador para que visite un sitio web malicioso controlado por el atacante a través de SSL-VPN.

Las versiones de FortiOS y FortiProxy afectadas por esta vulnerabilidad son las siguientes:

- FortiOS 7.4 desde la versión 7.4.0 hasta la versión 7.4.1.
- FortiOS 7.2 desde la versión 7.2.0 hasta la versión 7.2.6.
- FortiOS 7.0 desde la versión 7.0.0 hasta la versión 7.0.12.
- FortiOS 6.4 desde la versión 6.4.0 hasta la versión 6.4.14.
- FortiOS 6.2 desde la versión 6.2.0 hasta la versión 6.2.15.
- FortiOS 6.0 desde la versión 6.0 todas las versiones.
- FortiProxy 7.4 desde la versión 7.4.0 hasta la versión 7.4.1.
- FortiProxy 7.2 desde la versión 7.2.0 hasta la versión 7.2.7.
- FortiProxy 7.0 desde la versión 7.0.0 hasta la versión 7.0.13.
- FortiProxy 2.0 desde la versión 2.0 todas las versiones.
- FortiProxy 1.2 desde la versión 1.2 todas las versiones.
- FortiProxy 1.1 desde la versión 1.1 todas las versiones.
- FortiProxy 1.0 desde la versión 1.0 todas las versiones.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-522: Insufficiently Protected Credentials

CVSS Base: **7.5**

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ninguno**

- **Interacción con el usuario**: Requerida
- **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 la vulnerabilidad CVE-2023-45590, Fortinet recomienda:

- Actualizar a FortiClientLinux 7.2.1 o superior
- Actualizar a FortiClientLinux 7.0.11 o superior

Para corregir la vulnerabilidad CVE-2023-45588, CVE-2024-31492 Fortinet recomienda:

- Actualizar a FortiClientMac 7.2.4 o superior
- Actualizar a FortiClientMac 7.0.11 o superior

Para corregir la vulnerabilidad CVE-2023-41677 Fortinet recomienda:

- En el caso de FortiOS 7.4, actualizar a FortiOS 7.4.2 o superior
- En el caso de FortiOS 7.2, actualizar a FortiOS 7.2.7 o superior
- En el caso de FortiOS 7.0, actualizar a FortiOS 7.0.13 o superior
- En el caso de FortiOS 6.4, actualizar a FortiOS 6.4.15 o superior
- En el caso de FortiOS 6.2, actualizar a FortiOS 6.2.16 o superior
- En el caso de FortiOS 6.0 se recomienda migrar a una versión corregida
- En el caso de FortyProxy 7.4, actualizar a FortyProxy 7.4.2 o superior
- En el caso de FortyProxy 7.2, actualizar a FortyProxy 7.2.8 o superior
- En el caso de FortyProxy 7.0, actualizar a FortyProxy 7.0.14 o superior
- En el caso de FortyProxy 2.0, migrar a una versión corregida
- En el caso de FortyProxy 1.2, migrar a una versión corregida
- En el caso de FortyProxy 1.1, migrar a una versión corregida
- En el caso de FortyProxy 1.0, migrar a una versión corregida

Para corregir la vulnerabilidad CVE-2024-23671 Fortinet recomienda:

- En el caso de FortiSandbox 4.4, actualizar a FortiSandbox 4.4.4 o superior
- En el caso de FortiSandbox 4.2, actualizar a FortiSandbox 4.2.7 o superior
- En el caso de FortiSandbox 4.0, actualizar a FortiSandbox 4.0.5 o superior

Para corregir la vulnerabilidad CVE-2024-21755, CVE-2024-21756 Fortinet recomienda:

- En el caso de FortiSandbox 4.4, actualizar a FortiSandbox 4.4.4 o superior
- En el caso de FortiSandbox 4.2, actualizar a FortiSandbox 4.2.7 o superior
- En el caso de FortiSandbox 4.0, actualizar a FortiSandbox 4.0.5 o superior

5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2023-45590.
- CVE-2023-45588.
- CVE-2024-31492.
- CVE-2023-41677.
- CVE-2024-23671.
- CVE-2024-21755.
- CVE-2024-21756.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY