Nro. Alerta:	AL-2025-016	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
TLP:	TLP:CLEAR	**ALERTAS DE SEGURIDAD**	V 1.1
Fecha:	21-abr-2025	**Fortinet FortiOS y FortiProxy**	Pág.: **1** of **6**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de Incidente: Información

Nivel de riesgo: Alto

II. ALERTA

Figura 1.- Vulnerabilidad - figura referencial

Fortinet lanza asesoramiento para una nueva técnica post-explotación para 3 vulnerabilidades conocidas en sus productos FortiOS y FortiProxy.

III. INTRODUCCIÓN

El equipo de trabajo de Fortinet PSIRT (es el encargado de gestionar la recepción, investigación y la divulgación publica de información sobre vulnerabilidad de seguridad de fortiNet), tiene conocimiento de que un atacante crea un archivo malicioso a partir de vulnerabilidades previamente explotadas, CVE-2024-21762, CVE-2023-27997 y CVE-2022-42475, dentro de los productos de FortiGate (firewall de próxima generación NGFW).

El PSIRT observo como un atacante aprovechó una vulnerabilidad conocida para lograr acceso de solo lectura a dispositivos vulnerables de FortiGate.

El atacante logra su objetivo mediante la creación de un link simbólico que conectaba el sistema de archivos de usuario con el sistema de archivos root en una carpeta utilizada para archivos de idioma de SSL-VPN. Esta modificación se llevó a cabo en el sistema de archivos de usuario con lo cual evitó su detección.

Las vulnerabilidades detectadas tienen su impacto en la ejecución no Autorizada de código o comandos.

CVE-2024-21762: La vulnerabilidad CWE-787, clasificada como escritura fuera de los límites, afecta al componente sslvpnd en FortiOS y FortiProxy. Esta falla puede ser explotada de forma remota y sin autenticación, permitiendo que un atacante ejecute código o comandos arbitrarios mediante el envío de peticiones HTTP especialmente diseñadas, lo cual representa un riesgo crítico de compromiso total del sistema afectado.

CVE-2023-27997: La vulnerabilidad CWE-122, identificada como un desbordamiento de búfer en la memoria heap, afecta la funcionalidad de autenticación previa del servicio SSL-VPN en FortiOS y FortiProxy. Esta falla puede ser explotada remotamente y sin necesidad de autenticación, permitiendo que un atacante ejecute código o comandos arbitrarios mediante solicitudes especialmente construidas, comprometiendo de forma crítica la integridad del sistema.

CVE-2022-42475: La vulnerabilidad CWE-122, clasificada como desbordamiento de búfer en la memoria heap, afecta al componente SSL-VPN de FortiOS. Esta falla permite a un atacante remoto y no autenticado ejecutar código o comandos arbitrarios mediante solicitudes especialmente diseñadas, lo que representa un riesgo severo para la confidencialidad, integridad y disponibilidad del sistema comprometido.

IV. VECTOR DE ATAQUE

Todas las vulnerabilidades registradas poseen un nivel de riesgo alto y están consideradas como vector de ataque de RED.

CVE-2024-21762: Puntuación 9.6 -
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:W/RC:C

CVE-2023-27997: Puntuación 9.2 -
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:X/RC:R

CVE-2022-42475: Puntuación 9.3 -
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C

V. IMPACTO

Afectación de producto por vulnerabilidades:

CVE-2024-21762:

- FortiOS 7.4.0 hasta 7.4.2
- FortiOS 7.2.0 hasta 7.2.6
- FortiOS 7.0.0 hasta 7.0.13
- FortiOS 6.4.0 hasta 6.4.14
- FortiOS 6.2.0 hasta 6.2.15
- FortiOS 6.0.0 hasta 6.0.17
- FortiProxy 7.4.0 hasta 7.4.2
- FortiProxy 7.2.0 hasta 7.2.8
- FortiProxy 7.0.0 hasta 7.0.14
- FortiProxy 2.0.0 hasta 2.0.13
- FortiProxy 1.2 todas las versiones
- FortiProxy 1.1 todas las versiones
- FortiProxy 1.0 todas las versiones

CVE-2023-27997:

- FortiOS-6K7K version 7.0.10
- FortiOS-6K7K version 7.0.5
- FortiOS-6K7K version 6.4.12
- FortiOS-6K7K version 6.4.10
- FortiOS-6K7K version 6.4.8
- FortiOS-6K7K version 6.4.6
- FortiOS-6K7K version 6.4.2
- FortiOS-6K7K version 6.2.9 through 6.2.13
- FortiOS-6K7K version 6.2.6 through 6.2.7
- FortiOS-6K7K version 6.2.4
- FortiOS-6K7K version 6.0.12 through 6.0.16
- FortiOS-6K7K version 6.0.10
- FortiProxy version 7.2.0 through 7.2.3
- FortiProxy version 7.0.0 through 7.0.9
- FortiProxy version 2.0.0 through 2.0.12
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions
- FortiOS version 7.2.0 through 7.2.4
- FortiOS version 7.0.0 through 7.0.11

- FortiOS version 6.4.0 through 6.4.12
- FortiOS version 6.2.0 through 6.2.13
- FortiOS version 6.0.0 through 6.0.16

CVE-2022-42475:

- FortiOS versión 7.2.0 hasta 7.2.2
- FortiOS versión 7.0.0 hasta 7.0.8
- FortiOS versión 6.4.0 hasta 6.4.10
- FortiOS versión 6.2.0 hasta 6.2.11
- FortiOS versión 6.0.0 hasta 6.0.15
- FortiOS versión 5.6.0 hasta 5.6.14
- FortiOS versión 5.4.0 hasta 5.4.13
- FortiOS versión 5.2.0 hasta 5.2.15
- FortiOS versión 5.0.0 hasta 5.0.14
- FortiOS-6K7K versión 7.0.0 hasta 7.0.7
- FortiOS-6K7K versión 6.4.0 hasta 6.4.9
- FortiOS-6K7K versión 6.2.0 hasta 6.2.11
- FortiOS-6K7K versión 6.0.0 hasta 6.0.14
- FortiProxy versión 7.2.0 hasta 7.2.1
- FortiProxy versión 7.0.0 hasta 7.0.7
- FortiProxy versión 2.0.0 hasta 2.0.11
- FortiProxy versión 1.2.0 hasta 1.2.13
- FortiProxy versión 1.1.0 hasta 1.1.6
- FortiProxy versión 1.0.0 hasta 1.0.7

VI. INDICADORES DE COMPROMISO

Presencia de archivos sospechosos en el sistema en CVE-2022-42475:

La existencia de estos artefactos en el sistema de archivos puede indicar una intrusión o manipulación maliciosa:

- /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 salientes a direcciones IP maliciosas:

Se ha identificado actividad de red anómala con intentos de conexión desde dispositivos FortiGate hacia las siguientes direcciones IP:

- 188.34.130.40:444
- 103.131.189.143:30080, 30081, 30443, 20443
- 193.36.119.61:8443, 444
- 172.247.168.153:8033
- 139.180.184.197
- 66.42.91.32
- 158.247.221.101
- 107.148.27.117
- 139.180.128.142
- 155.138.224.122
- 185.174.136.20

VII. RECOMENDACIONES:

- Es esencial actualizar todos los dispositivos FortiOS a las siguientes versiones para mitigar vulnerabilidades conocidas:

  - FortiOS 7.6.2
  - FortiOS 7.4.7
  - FortiOS 7.2.11
  - FortiOS 7.0.17
  - FortiOS 6.4.16
  - FortiProxy 7.4.3
  - FortiProxy 7.2.9
  - FortiProxy 7.0.14 o superior
  - FortiOS-6K7K versión 7.0.12 o superior
  - FortiOS-6K7K versión 6.4.13 o superior
  - FortiOS-6K7K versión 6.2.15 o superior
  - FortiOS-6K7K versión 6.0.17 o superior

- Es recomendable realizar una revisión exhaustiva de la configuración de todos los dispositivos FortiOS.

- Revise y desactive servicios no utilizados, como SNMP o HTTP, para reducir la superficie de ataque

- Restringa el acceso administrativo a direcciones IP específicas mediante la configuración de "trusted hosts".

- Configure MFA para todas las cuentas de administrador y acceso remoto, utilizando métodos como tokens de hardware o aplicaciones de autenticación.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

https://www.cisa.gov/news-events/alerts/2025/04/11/fortinet-releases-advisory-new-post-exploitation-technique-known-vulnerabilities

https://www.fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-activity

https://fortiguard.fortinet.com/psirt/FG-IR-24-015

https://www.fortiguard.com/psirt/FG-IR-23-097

https://www.fortiguard.com/psirt/FG-IR-22-398