| Nro. Alerta: | AL-2025-019 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert<br>V 1.1 |
|---|---|---|---|
| TLP: | TLP:CLEAR | | |
| Fecha: | 16-may-2025 | **FORTINET** (CVE-2024-45324 y CVE-2023-42788) | Pág.: **1** of **1** |

## I. DATOS GENERALES:

**Clase de alerta:** Vulnerabilidad
**Tipo de Incidente:** Información
**Nivel de riesgo:** Alta

## II. ALERTA

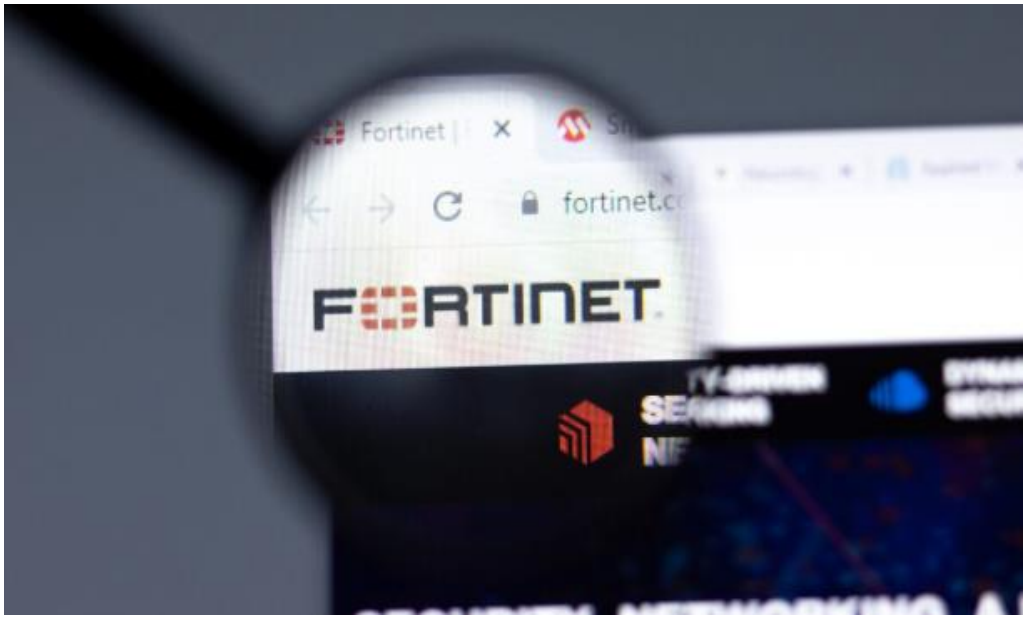


***Figura 1.-*** FORTINET - figura referencial

Nuevas vulnerabilidades han sido reveladas por el equipo PSIRT de FortiNet. CVE-2024-45324 una vulnerabilidad de cadena de formato controlada externamente [CWE-134] y CVE-2023-42788 permite la inyección de comandos arbitrarios [CWE-89].

## III. INTRODUCCIÓN

La vulnerabilidad CVE-2024-45324 afecta a los productos FortiOS, FortiProxy, FortiPAM, FortiSRA y FortiWeb, lo cual permite a un atacante con privilegios elevados ejecutar código o comandos no autorizados mediante solicitudes HTTP o HTTPS especialmente diseñadas.

La vulnerabilidad CVE-2023-42788 afecta a FortiManager y FortizAnalyzer permitiendo a un atacante local con privilegios elevados ejecutar comandos en el sistema operativo subyacente mediante la inyección de comandos a través de parámetros maliciosos por medio de la línea de comandos (CLI), las entradas de comandos no son validadas correctamente lo que permite obtener una shell interactiva como root.

## IV. VECTOR DE ATAQUE

Ambas vulnerabilidades poseen un nivel de riesgo alto y son de tipo RED:

**CVE-2024-45324:** puntuación 7.2 - CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

**CVE-2023-42788:** puntuación 8.8 - CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## V. IMPACTO

Afectación de productos por vulnerabilidades:

(CVE-2024-45324)

| Versión | Afectado | Solución |
|---|---|---|
| FortiOS 7.6 | No afectado | No aplicable |
| FortiOS 7.4 | 7.4.0 a 7.4.4 | Actualice a 7.4.5 o superior |
| FortiOS 7.2 | 7.2.0 a 7.2.9 | Actualice a 7.2.10 o superior |
| FortiOS 7.0 | 7.0.0 a 7.0.15 | Actualice a 7.0.16 o superior |
| FortiOS 6.4 | 6.4.0 a 6.4.15 | Actualice a 6.4.16 o superior |
| FortiOS 6.2 | 6.2.0 a 6.2.16 | Actualice a 6.2.17 o superior |
| FortiPAM 1.5 | No afectado | No aplicable |
| FortiPAM 1.4 | 1.4.0 a 1.4.2 | Actualice a 1.4.3 o superior |
| FortiPAM 1.3 | 1.3.0 a 1.3.1 | Actualice a 1.3.2 o superior |
| FortiPAM 1.2 | 1.2 todas las versiones | Migrar a una versión fija |
| FortiPAM 1.1 | 1.1 todas las versiones | Migrar a una versión fija |
| FortiPAM 1.0 | 1.0 todas las versiones | Migrar a una versión fija |
| FortiProxy 7.6 | 7.6.0 | Actualice a 7.6.1 o superior |
| FortiProxy 7.4 | 7.4.0 a 7.4.6 | Actualice a 7.4.7 o superior |
| FortiProxy 7.2 | 7.2.0 a 7.2.12 | Actualice a 7.2.13 o superior |
| FortiProxy 7.0 | 7.0.0 a 7.0.19 | Actualice a 7.0.20 o superior |
| FortiProxy 2.0 | No afectado | No aplicable |
| FortiSRA 1.5 | No afectado | No aplicable |
| FortiSRA 1.4 | 1.4.0 a 1.4.2 | Actualice a 1.4.3 o superior |
| FortiWeb 7.6 | 7.6.0 | Actualice a 7.6.1 o superior |
| FortiWeb 7.4 | 7.4.0 a 7.4.5 | Actualice a 7.4.6 o superior |
| FortiWeb 7.2 | 7.2.0 a 7.2.10 | Actualice a 7.2.11 o superior |
| FortiWeb 7.0 | 7.0.0 a 7.0.10 | Actualice a 7.0.11 o superior |

***Tabla 1.-*** *Afectación de Productos* – FORTINET (CVE-2024-45324)

(CVE-2023-42788)

| Versión | Afectado | Solución |
|---|---|---|
| FortiAnalyzer 7.4 | 7.4.0 | Upgrade to 7.4.1 or above |
| FortiAnalyzer 7.2 | 7.2.0 through 7.2.3 | Upgrade to 7.2.4 or above |
| FortiAnalyzer 7.0 | 7.0.0 through 7.0.8 | Upgrade to 7.0.9 or above |
| FortiAnalyzer 6.4 | 6.4.0 through 6.4.12 | Upgrade to 6.4.13 or above |
| FortiAnalyzer 6.2 | 6.2.0 through 6.2.11 | Upgrade to 6.2.12 or above |
| FortiAnalyzer-BigData 7.4 | Not affected | Not Applicable |
| FortiAnalyzer-BigData 7.2 | 7.2.0 through 7.2.5 | Upgrade to 7.2.6 or above |
| FortiAnalyzer-BigData 7.0 | 7.0 all versions | Migrate to a fixed release |
| FortiAnalyzer-BigData 6.4 | 6.4 all versions | Migrate to a fixed release |
| FortiAnalyzer-BigData 6.2 | 6.2 all versions | Migrate to a fixed release |
| FortiManager 7.4 | 7.4.0 | Upgrade to 7.4.1 or above |
| FortiManager 7.2 | 7.2.0 through 7.2.3 | Upgrade to 7.2.4 or above |
| FortiManager 7.0 | 7.0.0 through 7.0.8 | Upgrade to 7.0.9 or above |
| FortiManager 6.4 | 6.4.0 through 6.4.12 | Upgrade to 6.4.13 or above |
| FortiManager 6.2 | 6.2.0 through 6.2.11 | Upgrade to 6.2.12 or above |
| FortiManager Cloud 7.4 | Not affected | Not Applicable |
| FortiManager Cloud 7.2 | 7.2.1 through 7.2.3 | Upgrade to 7.2.4 or above |
| FortiManager Cloud 7.0 | 7.0.1 through 7.0.8 | Upgrade to 7.0.9 or above |
| FortiManager Cloud 6.4 | 6.4 all versions | Migrate to a fixed release |

***Tabla 2.-*** *Afectación de Productos* – FORTINET (CVE-2023-42788)

## VI. RECOMENDACIONES:

- Implementar segmentación de red para aislar los dispositivos Fortinet de redes públicas o no seguras.
- Aplicar segmentación de red para limitar el impacto de ataques internos.
- Habilitar logging detallado en los dispositivos Fortinet.
- Auditoría proactiva de las cuentas con privilegios administrativos.
- Realizar evaluaciones periódicas de seguridad para detectar configuraciones erróneas o vulnerabilidades no corregidas.
- Mantener copias de seguridad actualizada y verificada, garantizando la capacidad de recuperación ante incidentes de seguridad o fallos operativos.
- Restringir el acceso a CLI y GUI exclusivamente a usuarios autorizados y desde entornos controlados.

## VII. 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.

## VIII. REFERENCIAS:

https://www.cve.org/CVERecord?id=CVE-2024-45324

https://nvd.nist.gov/vuln/detail/CVE-2024-45324

https://www.fortiguard.com/psirt/FG-IR-24-325

https://www.securityweek.com/fortinet-patches-18-vulnerabilities/