Nro. Alerta:	AL-2025-014	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	10-abr-2025	FortiWeb (CVE-2025-25254)	Pág.: **1** of **3**

I. DATOS GENERALES:

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

II. ALERTA

Figura 1.- FortiWeb- figura referencial

CVE-2025-25254 - FortiWeb Endpoint vulnerabilidad CWE-22, es una falla de seguridad que permite a un atacante acceder a archivos o directorios fuera de la ubicación restringida prevista por el sistema.

III. INTRODUCCIÓN

Fortinet FortiWeb es un firewall que defiende las aplicaciones web y las API contra las amenazas OWASP Top-10, los ataques DDOS y los ataques de bots maliciosos entras sus capacidades incluyen detección de anomalías, descubrimiento y protección de API, mitigación de bots y análisis avanzado de amenazas para identificar las amenazas más críticas en todas las aplicaciones protegidas.

Se ha identificado una vulnerabilidad crítica en FortiWeb, clasificada bajo CWE-22 (Limitación Inadecuada de un Pathname a un Directorio Restringido). El fallo se localiza en ciertas funcionalidades no especificadas del sistema, donde el procesamiento inadecuado de entradas externas permite la explotación de un ataque de travesía de directorios (Path Traversal).

Una vez explotada la vulnerabilidad se utiliza datos proporcionados externamente (como entradas de usuario) para construir rutas de archivos o directorios dentro de una ubicación restringida. Sin embargo, no sanitiza correctamente caracteres especiales

como (../, %2e%2e%2f) en estas rutas, lo que permite a un atacante evadir las restricciones y acceder a ubicaciones fuera del directorio permitido.

IV. VECTOR DE ATAQUE

El ataque se lleva acabo de manera remota y es del tipo network CVSS:3.1/AV:**N**/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

V. IMPACTO

Esta vulnerabilidad se presenta como ejecución no autorizada de código o comandos y afecta a las versiones:

Versión	Afectación
FortiWeb 7.6	De 7.6.0 hasta 7.6.2
FortiWeb 7.4	De 7.4.0 hasta 7.4.6
FortiWeb 7.2	7.2 todas las versiones
FortiWeb 7.0	7.0 todas las versiones

VI. RECOMENDACIONES

Fortinet recomienda actualizar a las versiones:

- De 7.6 a versiones 7.6.3 o superior.
- De 7.4 a versiones 7.4.7 o superior.
- De las versiones 7.0 y 7.2 migrar a versiones corregidas (7.6.3 o 7.4.7 o superior).

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.cvedetails.com/cve/CVE-2025-25254/

https://www.cve.org/CVERecord?id=CVE-2025-25254

https://fortiguard.fortinet.com/psirt/FG-IR-24-474

https://vuldb.com/?id.303844

https://feedly.com/cve/CVE-2025-25254