Nro. Alerta:	AL-2025-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	11-jul-2025	Vulnerabilidad de SQL Injection en FortiWeb (CVE-2025-25257)	Pág.: **1** of **3**

I. DATOS GENERALES:

Clase de alerta: Informativo
Tipo de Incidente: SQL Injection
Nivel de riesgo: Alta

II. ALERTA

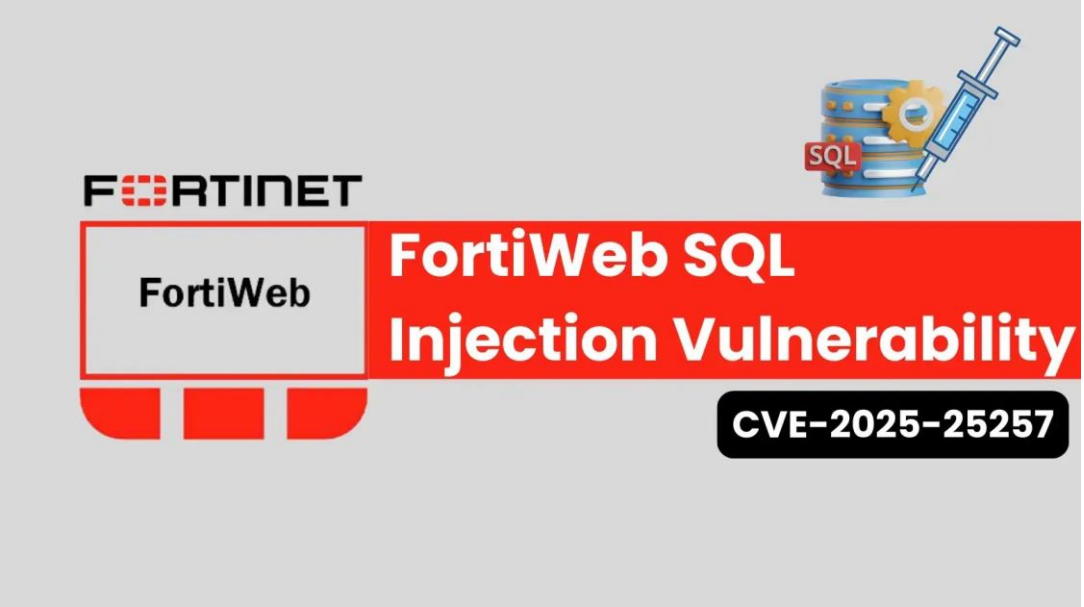

Figura 1.- Vulnerabilidad de SQL Injection en FortiWeb (CVE-2025-25257) - figura referencial

Una neutralización inadecuada de elementos especiales utilizado en el comando SQL (vulnerabilidad de "SQL Injection") [CWE-89] en FortiWeb (firewall de aplicaciones web (WAF) de Fortinet) permitiría a un atacante no autenticado ejecutar código o comandos SQL no autorizados mediante solicitudes HTTP o HTTPS manipuladas.

III. INTRODUCCIÓN

Una vulnerabilidad de seguridad crítica en el firewall de aplicaciones web FortiWeb de Fortinet, identificada como CVE-2025-25257, que permite a un atacante no autenticado ejecutar comandos SQL maliciosos a través de la interfaz gráfica de usuario del dispositivo.

Basado en CWE-89 que se refiere a una neutralización inadecuada de elementos especiales en comandos SQL (SQL Injection), con lo cual el atacante inserta código SQL malicioso a través de entradas no validadas (formularios, URLs, etc.), el sistema

ejecuta ese código como parte de una consulta a la base de datos y devuelve un resultado query que termina como robo de datos, borrado de tablas, escalada de privilegios, etc.

IV. VECTOR DE ATAQUE

Esta vulnerabilidad posee una severidad CRITICAL con una puntación CVSSv3 de 9.6 tipo /AV:N NETWORK

V. IMPACTO

El impacto de la explotación exitosa de esta vulnerabilidad incluye la capacidad de ejecutar código o comandos no autorizados en los sistemas afectados.

Esto podría conducir a un compromiso completo del sistema, exfiltración de datos, interrupción del servicio o movimiento lateral dentro de la infraestructura de la red.

Los productos y versiones afectados son los siguientes:

Version	Afectado
FortiWeb 7.6	Version 7.6.0 a 7.6.3
FortiWeb 7.4	Version 7.4.0 a 7.4.7
FortiWeb 7.2	Version 7.2.0 a 7.2.10
FortiWeb 7.0	Version 7.0.0 a 7.0.10

Tabla 1.- Versiones afectadas - Vulnerabilidad de SQL Injection en FortiWeb (CVE-2025-25257)

VI. INDICADORES DE COMPROMISOS

Hasta la fecha de elaboración de esta alerta, no se han publicado Indicadores de Compromiso (IoCs) específicos asociados a la explotación de esta vulnerabilidad. Tampoco se ha reportado la existencia de exploits públicos conocidos, debido a que la vulnerabilidad es reciente.

VII. RECOMENDACIONES:

- Como medida temporal, los administradores pueden deshabilitar la interfaz administrativa HTTP/HTTPS para reducir la superficie de ataque hasta que se complete la aplicación de los parches.
- Se recomienda a las organizaciones que utilicen FortiWeb en versiones afectadas aplicar las actualizaciones a las siguientes versiones:

Versión	Solución
FortiWeb 7.6	Actualizar a 7.6.4 o superior
FortiWeb 7.4	Actualizar a 7.4.8 o superior
FortiWeb 7.2	Actualizar a 7.2.11 o superior
FortiWeb 7.0	Actualizar a 7.0.11 o superior

Tabla 2.-Actulizacion de Versiones - Vulnerabilidad de SQL Injection en FortiWeb (CVE-2025-25257)

- Las organizaciones deben implementar medidas de seguridad adicionales, como la segmentación de red, los controles de acceso y el monitoreo continuo para detectar posibles intentos de explotación mientras se implementan parches.

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:

FORTIGUARD LABS (2025) https://fortiguard.fortinet.com/psirt/FG-IR-25-151

CVE MITRE https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-25257

TENABLE https://www.tenable.com/cve/CVE-2025-25257

GBHACKERS. (2025) https://gbhackers.com/fortiweb-sql-injection-vulnerability/

INSTITUTO NACIONAL DE CIBERSEGURIDAD (2025) https://www.incibe.es/incibe-cert/alerta-temprana/avisos/inyeccion-sql-en-fortiweb-de-fortinet

CIS CENTER FOR INTERNET SECURITY https://www.cisecurity.org/advisory/a-vulnerability-in-fortiweb-could-allow-for-sql-injection_2025-063