Alerta de

Seguridad

Vulnerabilidad Crítica Detectada en FortiWeb

COLCERT AL-20250718-066

TLP:CLEAR

Se ha identificado una vulnerabilidad que afecta a la aplicación de **FortiWeb**. Este es un sistema de seguridad que es utilizado por múltiples entidades para proteger sus **aplicaciones web** y **APIs**. Esta falla, identificada con el código CVE-2025-25257, está clasificada por la NIST como crítica y permite a cibercriminales tomar el control de sistemas sin necesidad de usuario ni contraseña. El ataque se realiza una operación de SQL Injection, que es una forma de engañar al sistema para que ejecute comandos maliciosos. Este boletín presenta un análisis técnico detallado por severidad, **incluye las técnicas MITRE ATT&CK asociadas a cada caso, y proporciona buenas prácticas y recomendaciones concretas para su mitigación.**

Consolidado de Vulnerabilidades por Severidad

Criticidad	Descripción	Impacto
Crítica	Acceso al sistema sin autenticación usando SQL Injection	Compromiso total del sistema, robo o manipulación de datos, ejecución de malware, persistencia.

Vulnerabilidad Crítica Identificada

CVE	Producto	Tipo	Impacto	Acción recomendada
CVE-2025-25257	Fortinet FortiWeb version 7.6.0 hasta 7.6.3, 7.4.0 a la 7.4.7, 7.0.0 a la 7.0.10	Envío de comandos SQL por peticiones HTTP o HTTPS.	Control del sistema a través de RCE (Remote Command Execution) sin autenticación	Actualizar a la versión más reciente
				Desactivar el acceso al panel del administrador

Riesgo Operativo Asociado:

La vulnerabilidad crítica identificada afecta a la disponibilidad del servicio web que se esté protegiendo, afecta a la confidencialidad ya que se puede acceder a credenciales y registros internos y al estar expuesto podría haber persistencia por parte del atacante. **Estas fallas representan un riesgo severo para la confidencialidad, integridad y disponibilidad de los datos, y pueden servir como punto inicial para ataques más amplios contra entornos corporativos o institucionales.**

Técnicas MITRE ATT&CK Asociadas (Críticas)

Técnica	Código	Descripción técnica
Explotación para acceso inicial	T1190	Se explota directamente la vulnerabilidad en un servicio expuesto de FortiWeb para obtener acceso al sistema sin credenciales.
Eliminación de logs e indicadores	T1070	Eliminación de rastros para evitar ser detectado
Intérprete de scripts y comandos	T1059	Abuso de la Shell del sistema operativo en el dispositivo de FortiWeb una vez conseguido el acceso inicial, con el fin de ejecutar acciones maliciosas

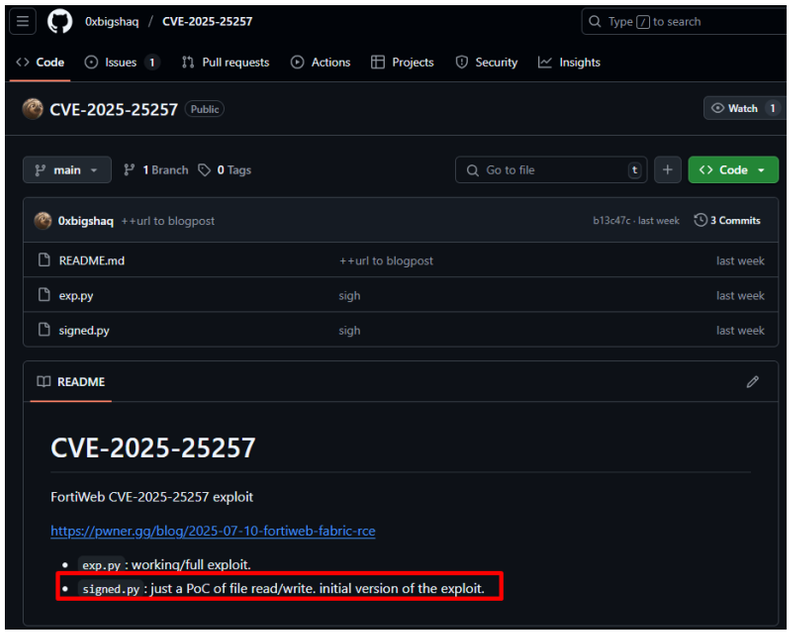
Validación de la vulnerabilidad

Explotación de la vulnerabilidad

A continuación, se evidencian rutas del repositorio de GitHub que muestran versiones para la explotación de la CVE-2025-25257.

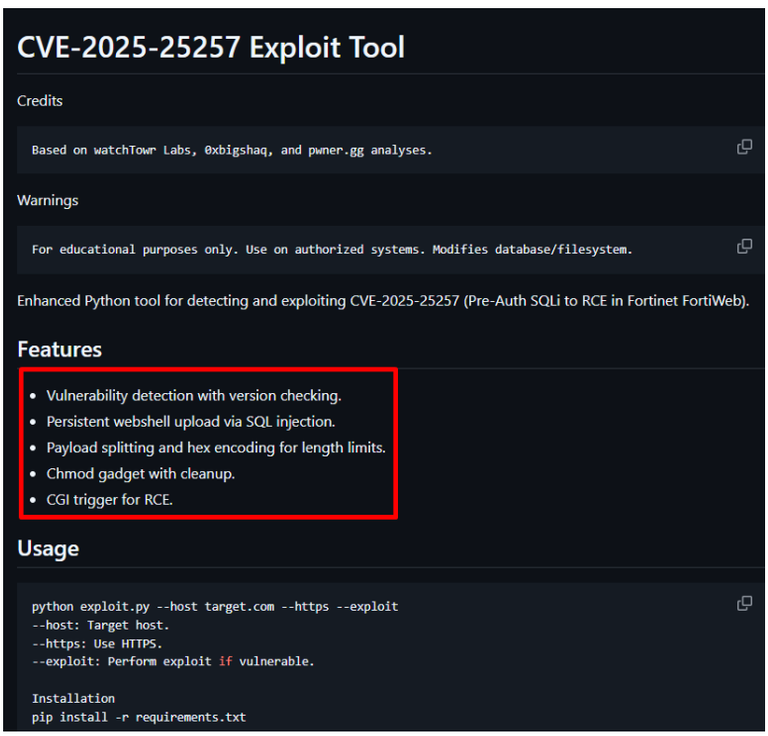
En el archivo signed.py se encontrará las pruebas de concepto de explotación a nivel inicial: :https://github.com/0xbigshaq/CVE-2025-25257

Figura 1. pruebas de concepto de explotación a nivel inicial



Fuente: https://github.com/0xbigshaq/CVE-2025-25257

Figura 2. fragmento de código que toma ventaja de la vulnerabilidad CVE-2025-25257.



Fuente: https://github.com/adilburaksen/CVE-2025-25257-Exploit-Tool

En la siguiente rura encontraremos el fragmento de código que toma ventaja de la vulnerabilidad CVE-2025-25257.

https://github.com/adilburaksen/CVE-2025-25257-Exploit-Tool

Buenas prácticas para mitigación

Figura 3. Alerta Crítica

Fuente: https://x.com/cycuramx/status/1945523824599945374?s=48&t=mDtpELQGEQ6lqu4xhesDzw

Solución y mitigaciones disponibles

- Aplicar actualizaciones de seguridad a las versiones parcheadas como: FortiWeb 7.6.4, FortiWeb 7.4.8, FortiWeb 7.0.11.
- Restringir y manejar el control de accesos al panel del administrador.
- Mantener constante monitoreo con el fin de detectar actividades sospechosas, en especial en las rutas de archivos **/cgi-bin/ml-draw.py**
- Control de acceso por medio de listas de Ips autorizadas.
- Evitar aplicar reglas generales o por defecto en las WAF.

Mitigaciones MITRE

Mitigación mitre	Código	Relevancia
Update Software	M1051	Aplicar los parches recomendados por Fortinet (versión 7.6.4+, etc.) es la acción más directa para eliminar la vulnerabilidad.
Exploit Protection	M1050	Ayuda a detectar y bloquear intentos de explotación activos mediante firmas o patrones conocidos.
Network Segmentation	M1030	Evita que un atacante que comprometa FortiWeb tenga acceso lateral a otros sistemas críticos.
Audit	M1047	La revisión de logs permite detectar actividad sospechosa y responder a tiempo.
Software configuration	M1054	Asegurar que el sistema esté correctamente configurado, deshabilitando módulos innecesarios.

Recomendaciones NO técnicas

- Asegura un procedimiento rápido de actualizaciones a los activos críticos de la organización.
- Capacitación continua del manejo de incidentes, con el fin de saber actuar frente alertas como el caso de FortiWeb.
- Promover que los usuarios y técnicos reporten comportamientos extraños o lentitud en sistemas críticos, lo que podría indicar actividad maliciosa no detectada aún.

Fuentes Oficiales

Bases de datos y catálogos de vulnerabilidades:

NIST National Vulnerability Database (NVD)
https://nvd.nist.gov/vuln/detail/CVE-2025-25257
Fuente principal de CVEs con detalles técnicos, puntajes CVSS y vectores de ataque.

MITRE CVE System
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-25257
Repositorio oficial de identificadores CVE y sus descripciones estandarizadas.

CISA KEV Catalog (Known Exploited Vulnerabilities)
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
Lista priorizada de vulnerabilidades con explotación activa confirmada

GitHub
https://github.com/0xbigshaq/CVE-2025-25257
Repositorio de proyectos colaborativos de software