Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

PARCHE CRÍTICO DE FORTIWEB: FALLA PERMITE RCE PRE-AUTENTICACIÓN Y REQUIERE ATENCIÓN INMEDIATA

14/ 07 / 2025

CONTENIDO

INTRODUCCIÓN

Recientemente se dio a conocer una nueva vulnerabilidad para FortiWeb, Esta se trata de una vulnerabilidad de SQL injection, en módulo de Fabric Connector de FortiWeb. Es no autenticada, esto significa que un atacante puede explotar la falla sin credenciales al enviar peticiones HTTP/HTTPS manipuladas.

PARCHE CRÍTICO DE FORTIWEB: FALLA PERMITE RCE PRE-AUTENTICACIÓN Y REQUIERE ATENCIÓN INMEDIATA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_07_14_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	14/07/2025
Es día cero (0 day):	No

RESUMEN

Recientemente se dio a conocer una nueva vulnerabilidad para FortiWeb, Esta se trata de una vulnerabilidad de SQL injection, en módulo de Fabric Connector de FortiWeb. Es no autenticada, esto significa que un atacante puede explotar la falla sin credenciales al enviar peticiones HTTP/HTTPS manipuladas.

¿Qué es FortiWeb?

FortiWeb es un firewall de aplicaciones web (WAF) utilizado para proteger aplicaciones web y APIs contra ataques como cross-site scripting, inyección SQL, y explotación de vulnerabilidades conocidas (OWASP Top 10).

Se le coloco una criticidad de CVSS: 9.8 siendo esta una falla critica, por lo cual se recomiendas hacer las actualizaciones de inmediato.

¿Cómo funciona el exploit?

El problema radica en cómo FortiWeb maneja los tokens de autorización que se reciben en peticiones HTTP, por ejemplo, en el encabezado Authorization: Bearer …

En lugar de validar correctamente el valor del token, el sistema lo inserta directamente en una consulta SQL, sin sanitizarlo ni usar parámetros seguros.

Un atacante envía una petición al endpoint vulnerable (por ejemplo, **/api/fabric/device/status**) usando un Authorization header con token malicioso tipo:

```
Authorization: Bearer AAAAAA'or'1'='1
```

Este token es insertado directamente en una consulta SQL, provocando la inyección. La vulnerabilidad permite usar comandos como:

```
SELECT … INTO OUTFILE '/path/to/file.pth' …
```

Para escribir un archivo. pth en el sistema de **Python**, potencialmente con privilegios elevados.
Luego, un script Python legítimo (como ml-draw.py) carga ese archivo. pth, lo que resulta en **ejecución remota de código** (RCE) como root.

Algunos investigadores ya han publicado pruebas de concepto completamente funcionales.

¿Cuáles son las versiones afectadas?

- 0.0 hasta 7.0.10
- 2.0 hasta 7.2.10
- 4.0 hasta 7.4.7
- 6.0 hasta 7.6.3

¿Cuál es el impacto?

El atacante puede desplegar shells, modificar la configuración, instalar backdoors o propagar la intrusión. Afecta servidores expuestos a Internet que no hayan sido parcheados inmediatamente.

RECOMENDACIONES

Actualización urgente a las versiones corregidas:

- 7.6.4+, 7.4.8+, 7.2.11+, 7.0.11+

Mientras no sea posible actualizar:

- Desactivar la interfaz administrativa HTTP/HTTPS, limitando el acceso solo a redes internas.

NOTICIA COMPLETA

https://devel.group/blog/parche-critico-de-fortiweb-falla-permite-rce-pre-autenticacion-y-requiere-atencion-inmediata/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group