Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD CRÍTICA EN FORTIWEB PERMITE BYPASS TOTAL DE AUTENTICACIÓN

20/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Una nueva vulnerabilidad crítica descubierta en FortiWeb, el firewall de aplicaciones web de Fortinet, ha encendido las alarmas en la comunidad de ciberseguridad. El fallo, identificado como CVE-2025-52970 y apodado FortMajeure, permite a atacantes remotos evadir por completo los mecanismos de autenticación y suplantar usuarios legítimos, incluso con privilegios administrativos.

Aunque Fortinet lanzó un parche el 12 de agosto de 2025, el riesgo sigue siendo alto, ya que el investigador que descubrió la falla liberó una prueba de concepto parcial que demuestra el impacto real del exploit. Esto significa que los actores maliciosos ya cuentan con información suficiente para intentar desarrollar un ataque funcional, lo que hace urgente la actualización de los sistemas vulnerables.

VULNERABILIDAD CRÍTICA EN FORTIWEB PERMITE BYPASS TOTAL DE AUTENTICACIÓN

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

ID de alerta:	DSOC-CERT_2025_20_08_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	20/08/2025
Es día cero (0 day):	No

RESUMEN

Investigadores revelaron detalles de una vulnerabilidad crítica en FortiWeb, el firewall de aplicaciones web de Fortinet, que permite a atacantes remotos evadir completamente los mecanismos de autenticación. El fallo fue reportado de forma responsable a Fortinet y ya está registrado como CVE-2025-52970.

La vulnerabilidad, bautizada por el investigador como FortMajeure, fue corregida por Fortinet en su actualización publicada el 12 de agosto de 2025.

¿En qué consiste la falla?
El problema radica en un error de lectura fuera de los límites (out-of-bounds read) en el análisis de cookies de FortiWeb.
Al manipular el parámetro Era, el sistema entra en un estado en el que utiliza una clave secreta compuesta únicamente por ceros para el cifrado de sesiones y la firma HMAC.

Esto permite que un atacante pueda crear cookies de autenticación falsas y así suplantar cualquier usuario activo, incluyendo cuentas administrativas.

Requisitos para la explotación
Para explotar CVE-2025-52970, el atacante necesita que la víctima tenga una sesión activa. Posteriormente, debe forzar por fuerza bruta un campo numérico del cookie, validado por la función refresh_total_logins().

Aunque Fortinet calificó el fallo con un puntaje CVSS de 7.7 debido a la “alta complejidad de ataque”, en la práctica el proceso es simple :

- El rango del valor a adivinar es menor a 30.
- Esto significa que en menos de 30 intentos se puede obtener acceso exitoso.

Versiones afectadas y correcciones
El fallo afecta a las versiones 7.0 a 7.6 de FortiWeb. Fortinet publicó las actualizaciones seguras:

- FortiWeb 7.6.4 y posteriores
- FortiWeb 7.4.8 y posteriores
- FortiWeb 7.2.11 y posteriores
- FortiWeb 7.0.11 y posteriores

La compañía aclaró que FortiWeb 8.0 no se ve impactado, por lo que no requiere medidas adicionales.

Riesgos y recomendaciones
Aunque los investigadores compartieron únicamente una PoC parcial, que demuestra la suplantación de un administrador en un endpoint REST, aún no ha liberado el exploit completo. Su intención es dar a los

administradores de sistemas tiempo para aplicar los parches antes de que la comunidad de atacantes pueda armar una cadena de explotación completa.

Sin embargo, los expertos advierten que el riesgo es altamente crítico:

- Los atacantes siguen de cerca estas publicaciones.
- La complejidad real del ataque es baja.

La explotación permite acceso total a FortiWeb, con posibilidad de controlar la configuración y acceder a la CLI del sistema.

Conclusión
Dado que Fortinet no ha publicado medidas de mitigación alternativas, la única protección efectiva es actualizar de inmediato a las versiones corregidas.

Las organizaciones que utilicen FortiWeb deben priorizar este parcheo en sus planes de gestión de vulnerabilidades, ya que la liberación del exploit completo es solo cuestión de tiempo.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-critica-en-fortiweb-permite-bypass-total-de-autenticacion/

CONTACTOS DE SOPORTE

Correo electrónico: cti@devel.group

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/