Alerta

Técnica

Vulnerabilidad Crítica Detectada en FortiWeb

COLCERT AL-20251118 - 083

TLP:CLEAR

Resumen Ejecutivo:

Se identificó que la vulnerabilidad **CVE-2025-64446** en **FortiWeb** está siendo explotada activamente, incluida en el catálogo de vulnerabilidades explotadas conocidas de CISA, lo que evidencia un riesgo inmediato para organizaciones que mantienen versiones sin parchear. Esta falla permite eludir la autenticación y otorgar control administrativo del WAF, facilitando la modificación de políticas, la instalación de persistencia y el potencial movimiento lateral hacia sistemas internos.

NIVEL DE RIESGO

ALTO

Considerando el uso de FortiWeb en sectores críticos, existe una alta probabilidad de que los intentos de explotación continúen y evolucionen hacia campañas más amplias en el corto plazo. De no implementarse medidas preventivas, se prevén impactos operacionales y reputacionales significativos, especialmente para infraestructuras expuestas a internet. Este análisis busca anticipar estos posibles escenarios y apoyar la toma de decisiones estratégicas para mitigar riesgos emergentes.

Vulnerabilidad identificada

CVE	Producto afectado	Score CVSS	Descripción
CVE-2025-64446	**FortiWeb** versiones: 8.0.0 → 8.0.1 (parche: 8.0.2) 17.6.0 → 7.6.4 (parche: ≥ 7.6.5) 7.4.0 → 7.4.9 (parche: ≥ 7.4.10) 7.2.0 → 7.2.11 (parche: ≥ 7.2.12) 7.0.0 → 7.0.11 (parche: ≥ 7.0.12)	**9.8 (Crítico)**	Permite a un ciberdelincuente no autenticado enviar peticiones HTTP/HTTPS especialmente manipuladas para ejecutar comandos administrativos, incluyendo la creación de cuentas admin, accediendo tanto al panel web de gestión como al CLI WebSocket.

¿Qué ha indicado Fortinet?

Fortinet publicó un aviso oficial a través de FortiGuard en el que registra la falla como **CVE-2025-64446**, la describe como una vulnerabilidad de *relative path traversal* que puede permitir a un atacante no autenticado ejecutar comandos administrativos y **confirma que han observado explotación en el ciberespacio**. **Fortinet** insta a los administradores a aplicar de inmediato las actualizaciones suministradas para las ramas afectadas y, como mitigación temporal cuando no sea posible parchear de inmediato, a restringir o aislar el acceso al panel de administración (evitar exposiciones HTTP/HTTPS públicas) y revisar la existencia de cuentas administrativas no autorizadas y cambios en la configuración.

¿Cómo aprovechan los ciberdelincuentes esta vulnerabilidad?

- **Envío de solicitudes HTTP/HTTPS especialmente manipuladas**: los ciberdelincuentes envían peticiones hacia el servicio web de administración del FortiWeb, utilizando rutas modificadas de forma maliciosa. El objetivo es engañar al sistema para que cargue componentes internos que normalmente requieren autenticación.

- **Bypass del mecanismo de autenticación**: a través del path traversal, el FortiWeb termina procesando solicitudes como si provinieran de un usuario legítimo con privilegios elevados. Esto permite al atacante acceder a funcionalidades administrativas sin credenciales válidas.

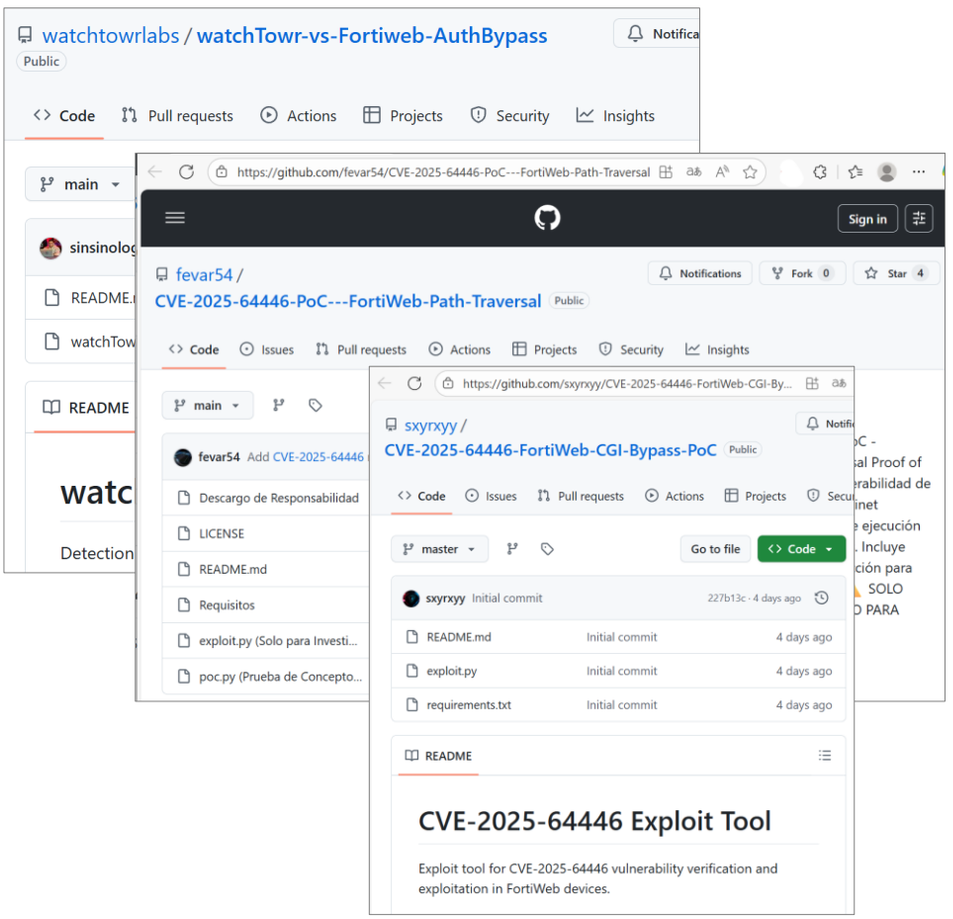
- **Ejecución de funciones administrativas**: una vez logrado el bypass, los actores de amenaza pueden invocar acciones internas del sistema, tales como administración de cuentas, acceso al WebSocket CLI, visualización o modificación de configuraciones sensibles. Esta fase transforma una falla de acceso en un control efectivo sobre el panel administrativo del WAF.

- **Creación de cuentas administrativas falsas**: en la explotación real observada, uno de los principales objetivos es la creación de cuentas administrativas no autorizadas. Estas cuentas permiten persistencia en el dispositivo, control total sobre la configuración del WAF, la posibilidad de desactivar reglas de seguridad o introducir configuraciones que permitan futuras intrusiones.

- **Posible uso del FortiWeb comprometido como punto de pivote**: una vez que los atacantes controlan el WAF pueden ocultar o manipular registros, deshabilitar protecciones, permitir tráfico malicioso hacia sistemas internos, o utilizar el dispositivo para un movimiento lateral. Esto convierte a un equipo diseñado para proteger la infraestructura en un activo utilizado para comprometerla.

En fuentes abiertas ya se encuentran disponibles diversas **pruebas de concepto** (PoC) para la explotación de la vulnerabilidad **CVE-2025-64446**, incluyendo *scripts* de bypass de autenticación y herramientas que permiten validar y reproducir el comportamiento descrito en los reportes oficiales.

Plataformas como GitHub y laboratorios de investigación independientes han publicado PoC funcionales que facilitan la verificación de sistemas vulnerables, lo cual incrementa la probabilidad de que actores maliciosos adopten rápidamente estos métodos en nuevas campañas de explotación.



Impacto para Colombia y la región

- **Sectores afectados**: financiero, salud, gobierno, TIC, energía, comercio, educación y servicios gestionados de TI.
- **Riesgo alto**: el riesgo es elevado debido a que la vulnerabilidad CVE-2025-64446 está siendo explotada activamente y permite acceso administrativo sin autenticación. La disponibilidad de PoC públicas y la amplia adopción de FortiWeb en la región incrementan la probabilidad de ataques exitosos en entornos productivos.
- **Posibles consecuencias**: desactivación o manipulación de reglas de seguridad, creación de cuentas administrativas no autorizadas, pérdida de integridad en la configuración del WAF, exposición de servicios internos, interrupción de operaciones, acceso no autorizado a información sensible, movimientos laterales hacia infraestructura crítica y debilitamiento de mecanismos de defensa perimetral.
- **Implicaciones en seguridad digital**: esta vulnerabilidad puede transformar un dispositivo de protección en un punto de entrada para actores maliciosos, afectando la confianza en la infraestructura perimetral. Además, obliga a las organizaciones a acelerar procesos de parcheo, fortalecer controles de acceso al panel de administración, implementar monitoreo de integridad y revisar la arquitectura de exposición de servicios críticos. Su explotación refuerza la necesidad de modelos de defensa en profundidad y de una capacidad regional de respuesta más coordinada y oportuna.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Exploit Public-Facing Application	**T1190**	Explotación de una aplicación o servicio expuesto a Internet para obtener acceso inicial, corresponde al vector de atacar el panel web de administración de FortiWeb mediante la vulnerabilidad.
Create Account	**T1136**	Creación de cuentas (local, dominio o *cloud*) por parte del ciberdelincuente para mantener acceso y persistencia.
Valid Accounts	**T1078**	Uso o abuso de cuentas válidas (incluye cuentas creadas o credenciales comprometidas) para autenticarse y moverse dentro del entorno.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Actualizar software	**M1051**	Aplicar de inmediato los parches y versiones publicadas por Fortinet elimina la vulnerabilidad en la raíz, mitigando directamente el vector de explotación y evitando que PoC públicas sean efectivas contra instancias parcheadas.
Escaneo de vulnerabilidades	**M1016**	Escanear sistemáticamente los perímetros y dispositivos de gestión permite identificar FortiWeb con versiones vulnerables y acelerar la remediación.
Gestión de cuentas privilegiadas	**M1026**	Limitar, controlar y auditar la creación y uso de cuentas administrativas, reduce el impacto si un atacante logra crear o abusar de cuentas admin.

Soluciones y mitigaciones disponibles

- **Aplicar de inmediato las actualizaciones oficiales publicadas por Fortinet**, instalando las versiones corregidas que eliminan la vulnerabilidad y reducen completamente el vector de explotación identificado contra FortiWeb expuesto a Internet. Establecer un esquema de gestión de vulnerabilidades de alta severidad que permita priorizar y acelerar el proceso de parcheo en tecnologías perimetrales como WAF, firewalls o VPN. Esto incluye definir ventanas de mantenimiento ágiles, criterios de criticidad y responsables claros de aprobación y ejecución.

- **Reducir la dependencia de un único control de seguridad** adoptando una arquitectura de capas que incluya microsegmentación, EDR, monitoreo avanzado, Zero Trust y controles de acceso robustos. Esto limita el impacto si uno de los dispositivos de protección es comprometido.

- **Verificar el estado de versión** de todos los dispositivos FortiWeb en la infraestructura, **priorizando aquellos accesibles desde Internet,** para identificar equipos vulnerables y asegurar una gestión adecuada del ciclo de parches.

- Restringir el acceso administrativo al panel de gestión de FortiWeb mediante **control estricto de IP permitidas**, uso de VPN corporativa y segmentación de red, minimizando la superficie expuesta a posibles atacantes.

- **Implementar autenticación multifactor** (MFA) para todas las cuentas administrativas que gestionen FortiWeb, reduciendo el riesgo de compromiso incluso si un actor obtiene credenciales válidas.

- **Monitorear los registros del dispositivo en busca de eventos anómalos**, tales como intentos repetidos de autenticación, creación de cuentas no autorizadas o cambios inesperados en la configuración. Además revisar todas las cuentas con roles administrativos configuradas en FortiWeb y eliminar aquellas que sean innecesarias o sospechosas, asegurando el principio de mínimo privilegio.

- Endurecer la configuración del dispositivo siguiendo las guías de hardening de Fortinet, deshabilitando servicios innecesarios, reforzando controles de acceso y aplicando políticas seguras por defecto.

- **Realizar escaneos de vulnerabilidades frecuentes** sobre los activos expuestos, incluyendo FortiWeb, para identificar rápidamente configuraciones inseguras o equipos que no hayan sido actualizados.

Fuentes

Fortinet Inc., 14 noviembre 2025, PSIRT Advisory: FG-IR-25-910 – FortiWeb Relative Path Traversal Vulnerability, fuente del proveedor.
https://fortiguard.fortinet.com/psirt/FG-IR-25-910

National Institute of Standards and Technology (NIST), 14 noviembre 2025, CVE-2025-64446 Detail, base de datos de vulnerabilidades (NVD).
https://nvd.nist.gov/vuln/detail/CVE-2025-64446

Cybersecurity News, 14 noviembre 2025, FortiWeb WAF Vulnerability Explote in the Wild, medio de noticias de ciberseguridad.
https://cybersecuritynews.com/fortiweb-waf-vulnerability-exploited-in-the-wild/

Fortinet Inc., 15 julio 2025, FortiWeb 8.0.0 Administration Guide – Hardening Security, documentación técnica del fabricante.
https://docs.fortinet.com/document/fortiweb/8.0.0/administration-guide/121009/hardening-security