Boletín de alerta

Boletín Nro.:
Fecha de publicación: 26/08/2025
Tema: Alerta 2025-72 Vulnerabilidad crítica en FortiWeb (WAF)
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Fortinet FortiWeb (WAF)** en las versiones:
  - 7.6.0 hasta 7.6.3
  - 7.4.0 hasta 7.4.7
  - 7.2.0 hasta 7.2.10
  - 7.0.0 hasta 7.0.10

Descripción

El equipo de Fortinet ha identificado y publicado una nueva vulnerabilidad de manejo incorrecto de parámetros en Fortinet FortiWeb, identificada como CVE-2025-52970 con un CVVS de 7.7.

La vulnerabilidad se debe a una validación deficiente de un parámetros de entrada en el FortiWeb, lo que permite a un atacante remoto y no autenticado, con información no pública sobre el dispositivo o el usuario, enviar solicitudes manipuladas para eludir restricciones de seguridad y obtener acceso administrativo.

Una vez explotada, el atacante podría iniciar sesión como un usuario legítimo, escalar privilegios y lograr acceso persistente al sistema, con potencial de ejecutar código malicioso. Fuentes también alertan: “un atacante podría lograr acceso persistente y potencialmente ejecución de código” si la vulnerabilidad es explotada

La existencia de un **exploit público (PoC)** confirmado incrementa el riesgo de explotación activa en entornos reales. La publicación del PoC y el aviso del **H-ISAC TLP White (18 de agosto de 2025)** advierten que la disponibilidad del exploit aumenta la probabilidad de explotación real.

Solución:

Fortinet ha publicado parches en el aviso FG?IR?25?448. **Actualizar de inmediato** todos los dispositivos FortiWeb afectados a versiones parcheadas.

Las versiones seguras disponibles son:

Versión Vulnerable (hasta)	Versión Segura (desde)
FortiWeb 7.6.0–7.6.3	**7.6.4 o superior**
FortiWeb 7.4.0–7.4.7	**7.4.8 o superior**
FortiWeb 7.2.0–7.2.10	**7.2.11 o superior**
FortiWeb 7.0.0–7.0.10	**7.0.11 o superior**

Acciones urgentes recomendadas

- En caso de no poder actualizar de forma inmediata, aplicar medidas temporales como bloquear acceso externo al dispositivo o restringir interfaces de administración hasta completar la actualización.
- Establecer monitoreo activo de logs y tráfico inusual que pueda indicar intentos de explotación.
- Implementar segmentación de red y controles de acceso adicionales.

Información adicional:

- https://pwner.gg/blog/2025-08-13-fortiweb-cve-2025-52970
- PSIRT | FortiGuard Labs
- https://nvd.nist.gov/vuln/detail/CVE-2025-52970