Boletín de alerta

Boletín Nro.:
Fecha de publicación: 14/11/2025
Tema: Alerta 2025-98 Vulnerabilidad 0-day en productos Fortinet
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Fortinet FortiWeb versiones anteriores a 8.0.2**
- **FortiWeb Manager**
- **Interfaces administrativas y WebSocket de FortiWeb**

Descripción

La vulnerabilidad identificada afecta a dispositivos **Fortinet FortiWeb**, específicamente a las interfaces de administración y a los componentes encargados de manejar solicitudes HTTP/HTTPS y WebSocket. Todo indica que el fallo está relacionado con una **omisión de autenticación combinada con un recorrido de rutas (path traversal)**, lo que permite a un atacante interactuar con componentes internos del sistema sin requerir credenciales válidas. **Más vale tarde que nunca: Fortinet publicó el comunicado oficial y asignó el CVE-2025-64446 (CVSS 9.1), confirmando la criticidad del hallazgo.**

Aunque inicialmente no existía una confirmación oficial por parte de Fortinet, diversos investigadores habían observado patrones muy similares al comportamiento del **CVE-2022-40684**, una vulnerabilidad histórica de bypass de autenticación en FortiOS, FortiProxy y FortiSwitchManager. Por ello, antes del anuncio oficial varios analistas etiquetaban esta falla como «similar a CVE-2022-40684». Con la publicación del nuevo CVE, se confirma la relación técnica, aunque se considera una vulnerabilidad distinta.

El atacante explota una falla en la validación de rutas posiblemente una combinación de codificación parcial y salto de directorios para acceder a un endpoint interno normalmente reservado para administradores autenticados. Se ha observado que los atacantes envían solicitudes manipuladas hacia una ruta alterada que utiliza codificación para evadir los controles de validación del sistema.

Esta ruta modificada provoca que el servidor interprete incorrectamente la ubicación real del recurso solicitado, redirigiendo la petición hacia un script interno (**fwbcgi**) que forma parte de los mecanismos administrativos del dispositivo. Una vez alcanzado este punto interno, el atacante envía una carga útil diseñada para **crear nuevas cuentas administrativas**, otorgándole control total sobre el dispositivo afectado.

Mitigación:

Fortinet indicó que la medida correcta para mitigar esta vulnerabilidad es actualizar a una versión corregida. Las versiones afectadas y sus respectivas soluciones son las siguientes: FortiWeb 8.0 (de 8.0.0 a 8.0.1) debe actualizarse a la versión 8.0.2 o superior; FortiWeb 7.6 (de 7.6.0 a 7.6.4) debe actualizarse a la versión 7.6.5 o superior; FortiWeb 7.4 (de 7.4.0 a 7.4.9) debe actualizarse a la versión 7.4.10 o superior; FortiWeb 7.2 (de 7.2.0 a 7.2.11) debe actualizarse a la versión 7.2.12 o superior; y FortiWeb 7.0 (de 7.0.0 a 7.0.11) debe actualizarse a la versión 7.0.12 o superior.

https://fortiguard.fortinet.com/psirt/FG-IR-25-910

Información adicional:

- https://cybersecuritynews.com/fortinet-fortiweb-vulnerability/
- https://www.rapid7.com/blog/post/etr-critical-vulnerability-in-fortinet-fortiweb-exploited-in-the-wild/
- https://www.pwndefend.com/2025/11/13/suspected-fortinet-zero-day-exploited-in-the-wild/
- https://x.com/DefusedCyber/status/1975242250373517373?s=20
- https://nvd.nist.gov/vuln/detail/cve-2022-40684
- *https://fortiguard.fortinet.com/psirt/FG-IR-25-910*
-