Boletín de alerta

Boletín Nro.: 38
Fecha de publicación: 15/04/2026
Tema: Alerta 2026-38 Vulnerabilidades críticas de RCE en Fortinet FortiSandbox
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Según los avisos de autoridades nacionales y Fortinet, las vulnerabilidades afectan principalmente a:

Producto	Versiones afectadas (principales)
FortiSandbox	4.4.0 – 4.4.8 (CVE-2026-39808, 39813)
FortiSandbox 5.0.x	5.0.0 – 5.0.5 (CVE-2026-39813)
FortiSandbox PaaS	Hasta 4.4.8 (CVE-2026-39808)
FortiSandbox Cloud	5.0.4 (CVE-2026-25836 – RCE autenticada)

Descripción

Se han revelado nuevas vulnerabilidades críticas en productos Fortinet, principalmente en FortiSandbox, destacando **CVE-2026-39808** y **CVE-2026-39813**, ambas con **CVSS 9.8–9.1 (críticas)**, que pueden permitir ejecución remota de código (RCE), escalada de privilegios y bypass de autenticación en entornos usados para analizar malware y archivos sospechosos. Dado que estos dispositivos suelen estar conectados a redes internas de alta sensibilidad, su compromiso puede convertirse en un punto de entrada privilegiado para los atacantes.

FortiSandbox es una solución de seguridad avanzada que analiza de forma aislada archivos y tráfico sospechoso para detectar malware y amenazas de día cero antes de que alcancen la red corporativa. Se despliega como producto independiente (appliance físico, máquina virtual o servicio en la nube) y se integra con otros dispositivos Fortinet —como FortiGate, FortiMail o FortiWeb— que le envían objetos a inspeccionar, por lo que la sandbox se administra y actualiza por separado dentro de la infraestructura de seguridad.

Detalle de las vulnerabilidades más críticas:

- **CVE-2026-39808 – OS Command Injection en FortiSandbox (Crítica)**:
  Vulnerabilidad de inyección de comandos del sistema operativo (CWE-78) en FortiSandbox y FortiSandbox PaaS hasta la versión 4.4.8. Un atacante remoto puede enviar peticiones manipuladas a

funciones específicas del producto y conseguir que se ejecuten comandos arbitrarios con privilegios elevados en el sistema subyacente, lo que puede conducir a un control completo del dispositivo.

- **CVE-2026-39813 – Path Traversal y RCE en FortiSandbox (Crítica)**:
  Fallo de *path traversal* en la API JRPC de FortiSandbox que permite a un atacante no autenticado eludir la autenticación y acceder a rutas internas del sistema. En combinación con otras funciones, este acceso puede aprovecharse para cargar o ejecutar código malicioso, obteniendo RCE y potencial escalada de privilegios en versiones 4.4.0–4.4.8 y también 5.0.0–5.0.5.

Fortinet también ha publicado avisos complementarios donde describe otros fallos adicionales (incluyendo vulnerabilidades de RCE autenticada en FortiSandbox Cloud, como **CVE-2026-25836**, que permiten a un usuario con perfil super-admin ejecutar comandos OS mediante peticiones HTTP especialmente construidas)

Solución:

Fortinet ha publicado **actualizaciones de seguridad para FortiSandbox, FortiSandbox PaaS y FortiSandbox Cloud**, que corrigen las vulnerabilidades de RCE, path traversal y command injection. Se recomienda:

- Actualizar FortiSandbox 4.4.x y 5.0.x a las últimas versiones disponibles indicadas en el advisory **FG-IR-26-112 / FG-IR-26-100** y boletines de producto de Fortinet.
  - https://www.fortiguard.com/psirt/FG-IR-26-100
  - https://fortiguard.fortinet.com/psirt/FG-IR-26-112
- En FortiSandbox Cloud, aplicar las mitigaciones y parches recomendados para la versión 5.0.4 y posteriores (especialmente frente a CVE-2026-25836).
  - https://docs.fortinet.com/document/fortisandbox/5.0.6/release-notes/82966/upgrade-information
- Restringir el acceso de red a las interfaces de administración y APIs de FortiSandbox, limitándolo a segmentos de gestión internos y aplicando controles de firewall y VPN adecuados.
  - https://docs.fortinet.com/document/fortisandbox/3.2.2/administration-guide/494405/update-the-fortisandbox-firmware
  - https://docs.fortinet.com/document/fortisandbox-private-cloud/3.1.0/fortisandbox-vm-on-vmware/519274/downloading-deployment-packages
- Revisar registros de la sandbox en busca de actividad anómala, comandos sospechosos o conexiones salientes inusuales, especialmente en periodos previos al parcheo.
- Documentación y parches oficiales se encuentran en el portal **FortiGuard PSIRT** (avisos FG-IR-26-112, FG-IR-26-100 y relacionados) y en las notas de versión de FortiSandbox.
  - https://www.fortiguard.com/psirt

Información adicional:

- https://www.theregister.com/2026/04/15/critical_fortinet_sandbox_bugs/
- https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2026-39813
- https://www.fortiguard.com/psirt/FG-IR-26-115

- https://fortiguard.fortinet.com/psirt/FG-IR-26-109
- https://fortiguard.fortinet.com/psirt/FG-IR-26-110
- https://fortiguard.fortinet.com/psirt/FG-IR-26-112
- https://www.fortiguard.com/psirt/FG-IR-26-100