Boletín de alerta

Boletín Nro.:
Fecha de publicación: 18/06/2026
Tema: Alerta 2026-66 Vulnerabilidades críticas en FortiSandbox y alerta sobre la campaña FortiBleed
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- FortiSandbox 4.4.0 a 4.4.8 (CVE-2026-39808, CVE-2026-39813, CVE-2026-25089)
- FortiSandbox 5.0.0 a 5.0.5 (CVE-2026-25089)
- FortiSandbox Cloud 5.0.4 a 5.0.5 (CVE-2026-25089)
- FortiSandbox PaaS 5.0.4 a 5.0.5 (CVE-2026-25089)

Nota: el aviso oficial de Fortinet indica que FortiSandbox 5.0 no está afectado por CVE-2026-39808, y que FortiSandbox PaaS 5.0 tampoco está afectado por este CVE.

Descripción

Fortinet publicó actualizaciones de seguridad para corregir tres vulnerabilidades críticas en **FortiSandbox** que permiten a atacantes remotos no autenticados ejecutar comandos arbitrarios, evadir mecanismos de autenticación y comprometer completamente los sistemas afectados mediante solicitudes HTTP especialmente diseñadas. Estas vulnerabilidades, identificadas como **CVE-2026-39813**, **CVE-2026-39808** y **CVE-2026-25089**, tienen una puntuación CVSS v3 de **9.1 (Crítico)** y ya cuentan con parches oficiales disponibles desde abril y junio de 2026.

Empresas de inteligencia de amenazas (Defused, SecurityWeek, Help Net Security, entre otras) han observado **explotación activa en Internet** de las tres fallas poco tiempo después de la publicación de los parches, lo que indica campañas contra appliances expuestos que no han sido actualizados. Aunque estas campañas se enmarcan en un contexto más amplio de ataques al ecosistema Fortinet, es importante aclarar que **las vulnerabilidades de FortiSandbox son un problema técnico distinto** de la campaña "FortiBleed", centrada en la filtración y abuso de credenciales en dispositivos FortiGate/SSL VPN.

A continuación, se detallan las vulnerabilidades más importantes en FortiSandbox:

- **CVE-2026-39808 – OS Command Injection a través de API (CVSS 9.1)**

Una vulnerabilidad de **OS Command Injection** en un endpoint de la API de FortiSandbox permite a un atacante remoto no autenticado ejecutar código o comandos arbitrarios mediante peticiones HTTP

especialmente construidas. La explotación exitosa puede derivar en **ejecución remota de código (RCE)** con alto impacto sobre la confidencialidad, integridad y disponibilidad del dispositivo.

- **CVE-2026-25089 – OS Command Injection en Web UI (CVSS 9.1)**

Una vulnerabilidad de tipo **Improper Neutralization of Special Elements used in an OS Command (CWE-78)** afecta a la interfaz web de FortiSandbox, FortiSandbox Cloud y FortiSandbox PaaS. Un atacante remoto no autenticado puede ejecutar comandos arbitrarios mediante peticiones HTTP manipuladas hacia la funcionalidad de inicio de sesiones VNC (start vnc), comprometiendo la plataforma subyacente. Defused ha observado intentos de explotación de esta vulnerabilidad, e incluso ha señalado que uno de los exploits detectados parece haber sido generado con ayuda de IA.

- **CVE-2026-39813 – Path Traversal / Authentication Bypass (CVSS 9.1)**

Una vulnerabilidad de **Path Traversal** en la interfaz JRPC API de FortiSandbox puede permitir a un atacante remoto **eludir los controles de autenticación** mediante solicitudes especialmente construidas. Dependiendo de la configuración del entorno, esta falla puede utilizarse para obtener acceso privilegiado y facilitar la explotación de otras vulnerabilidades o la ejecución de acciones administrativas no autorizadas. Tanto Defused como otros proveedores de inteligencia han reportado intentos activos de explotación de CVE-2026-39813 y CVE-2026-39808 en entornos reales, pocos días después de su divulgación inicial.

Aclaración sobre "FortiBleed"

Diversos informes públicos emplean el término **"FortiBleed"** para describir una **campaña de filtración y abuso de credenciales** que afecta principalmente a firewalls FortiGate y gateways SSL VPN, donde se ha observado la compilación de bases de datos con credenciales válidas para decenas de miles de dispositivos en más de 190 países.

Los atacantes han recopilado **configuraciones de FortiGate** expuestos, han extraído los hashes de contraseñas admins/VPN y los han crackeado offline con clusters de GPU, aprovechando que muchas contraseñas seguían almacenadas con **SHA-256 con salt**, más débil, incluso después de upgrades.

Fortinet y varios analistas remarcan que **FortiBleed "no tiene CVE"**: no es un zero-day nuevo, sino explotación a gran escala de credenciales obtenidas por leaks previos, fuerza bruta, password spraying y mala higiene (reuso, no rotación, falta de MFA, paneles expuestos).

Fortinet aclaró que no se trata de una vulnerabilidad nueva, sino de ataques de credential-stuffing y fuerza bruta contra dispositivos con contraseñas débiles o reutilizadas y sin MFA, mientras que en paralelo publicó parches para otras vulnerabilidades (como FortiSandbox), lo que generó confusión en algunos reportes iniciales

Si bien algunas piezas de inteligencia mencionan la explotación de vulnerabilidades en productos Fortinet (incluido FortiSandbox) en el mismo contexto, actualmente **no existe una evidencia técnica pública que vincule directamente** estos tres CVE de FortiSandbox con el dataset de credenciales conocido como FortiBleed. En este boletín tratamos las vulnerabilidades de **FortiSandbox** como un vector independiente, con mitigaciones específicas

Solución

Se recomiendan las siguientes acciones de forma inmediata sobre equipo FortiSandbox:

- CVE-2026-39808
  - FortiSandbox 5.0.0–5.0.5 Actualizar a 5.0.6 o superior.
  - FortiSandbox 4.4.0–4.4.8 Actualizar a 4.4.9 o superior.
- CVE-2026-25089
  - FortiSandbox 5.0.0–5.0.5 Actualizar a 5.0.6 o superior.
  - FortiSandbox 4.4.0–4.4.8 Actualizar a 4.4.9 o superior.
  - FortiSandbox Cloud 5.0.4–5.0.5 Actualizar a 5.0.6 o superior.
  - FortiSandbox PaaS 5.0.4–5.0.5 Actualizar a 5.0.6 o superior.
- CVE-2026-39813
  - FortiSandbox 5.0.0–5.0.5 Actualizar a 5.0.6 o superior.
  - FortiSandbox 4.4.0–4.4.8 Actualizar a 4.4.9 o superior.

Recomendaciones sobre FortiBleed

Antes de aplicar las medidas de contención, se recomienda verificar si la organización aparece en el dataset asociado a FortiBleed mediante el FortiBleed Checker de Hudson Rock, disponible en https://www.hudsonrock.com/fortinet. Esta herramienta gratuita permite consultar si dominios o activos de la organización figuran entre los dispositivos expuestos identificados públicamente, y varios reportes y organismos la citan como paso inicial de validación de impacto. Encontramos hasta ahora 82 dominios de empresas e instituciones mexicanas (50 privadas y 32 de gobierno).

Si crees que información de tus organización fue expuesta en la campaña FortiBleed recomendamos:

1. **Rotar todas las claves**
   Cambiar inmediatamente contraseñas de admins de FortiGate y de todos los usuarios de SSL VPN.
2. **Activar MFA en todo acceso remoto**
   Habilitar MFA obligatoria para administración y VPN; sin MFA, asumir credenciales comprometidas.
3. **Actualizar FortiOS a la última versión soportada**
   Llevar FortiGate a releases donde se corrigen fallos de auth bypass y se usan hashes PBKDF2, no SHA 256.
4. **Cerrar la consola de administración a Internet**
   Quitar HTTP/HTTPS/SSH de la zona pública o limitarlo a IPs de administración/jump hosts.
5. **Revisar logs de accesos sospechosos**
   Buscar logins de admin desde países extraños, horas inusuales o muchos intentos fallidos seguidos.
6. **Rotar credenciales también en AD si se usaron para VPN**
   Si cuentas AD se emplean en la SSL VPN, forzar cambio de contraseña y revisar actividad en AD.
7. **Revisar reglas de firewall/VPN**
   Confirmar que no se hayan creado túneles o accesos remotos que nadie reconoce.

Información adicional:

- Help Net Security Advisory
- Fortinet PSIRT FG-IR-26-100 (CVE-2026-39808)
- Fortinet PSIRT FG-IR-26-141 (CVE-2026-25089)
- The Hacker News – Active Exploitation of FortiSandbox Vulnerabilities
- SecurityWeek Analysis