Boletín de alerta

Boletín Nro.:
Fecha de publicación: 17/07/2026
Tema: Alerta 2026-73 Vulnerabilidades activamente explotadas Fortinet
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- · FortiSandbox 4.4.0 a 4.4.8
- · FortiSandbox 5.0.0 a 5.0.5
- · FortiSandbox Cloud 5.0.4 a 5.0.5
- · FortiSandbox PaaS 5.0.4 a 5.0.5

Descripción

La **Cybersecurity and Infrastructure Security Agency (CISA)** de los Estados Unidos incorporó dos vulnerabilidades críticas de **Fortinet FortiSandbox** a su catálogo de **Known Exploited Vulnerabilities (KEV)** tras confirmar su explotación activa. Como parte de la **Binding Operational Directive (BOD) 26-04**, las agencias federales estadounidenses deben aplicar las actualizaciones correspondientes **a más tardar el 19 de julio de 2026** para mitigar el riesgo de compromiso.

Aunque la directiva de CISA incorpora formalmente **CVE-2026-39808** y **CVE-2026-25089**, diversas firmas de inteligencia de amenazas observaron que los atacantes también están intentando explotar **CVE-2026-39813**, lo que indica campañas dirigidas contra múltiples fallas del producto.

FortiSandbox es una solución utilizada para el análisis dinámico de archivos y URLs sospechosos dentro del ecosistema **Fortinet Security Fabric**. Debido a su integración con firewalls, soluciones EDR, correo electrónico, SIEM y SOAR, un compromiso del appliance puede afectar múltiples controles de seguridad empresariales.

Las vulnerabilidades identificadas son:

CVE-2026-25089 – OS Command Injection (CVSS 9.8): Esta vulnerabilidad afecta la interfaz web de FortiSandbox, FortiSandbox Cloud y FortiSandbox PaaS. Un **atacante remoto no autenticado** puede enviar solicitudes HTTP especialmente diseñadas para **ejecutar comandos arbitrarios sobre el sistema operativo** del dispositivo comprometido.

CVE-2026-39813 – Path Traversal / Authentication Bypass (CVSS 9.1): Esta vulnerabilidad permite a un **atacante remoto manipular rutas** dentro de la interfaz JRPC API para eludir controles de autenticación y acceder a funcionalidades restringidas. En combinación con otras vulnerabilidades, puede facilitar la ejecución de código y el compromiso total del appliance.

CVE-2026-39808 – OS Command Injection (CVSS 9.1): Esta vulnerabilidad corresponde a una **inyección de comandos del sistema operativo** en una API de FortiSandbox. Un atacante remoto **no autenticado** puede enviar solicitudes HTTP especialmente diseñadas para ejecutar código o comandos arbitrarios sobre el dispositivo vulnerable.

Cuando Fortinet publicó inicialmente los parches en junio de 2026, indicó que **no existía evidencia de explotación activa**. Sin embargo, pocos días después, investigadores independientes y empresas de inteligencia de amenazas reportaron actividad maliciosa dirigida contra dispositivos vulnerables expuestos a Internet. Posteriormente, CISA confirmó la explotación activa al incorporar **CVE-2026-25089** y **CVE-2026-39813** al catálogo **KEV**, obligando a las agencias federales estadounidenses a corregirlas en un plazo reducido.

Diversos investigadores señalan que los atacantes están utilizando estas vulnerabilidades para comprometer dispositivos FortiSandbox expuestos y obtener ejecución remota de código, lo que convierte a los appliances —diseñados para analizar malware— en un punto de entrada hacia la infraestructura corporativa.

El 16 de junio de 2026 investigadores de **Defused** detectaron campañas activas dirigidas contra dispositivos FortiSandbox vulnerables, observando explotación de **CVE-2026-39808**, **CVE-2026-25089** y también intentos relacionados con **CVE-2026-39813**. Posteriormente, el 17 de julio de 2026, **CISA confirmó la explotación activa de CVE-2026-39808 y CVE-2026-25089**, incorporándolas al catálogo **Known Exploited Vulnerabilities (KEV)** y estableciendo un plazo acelerado para su remediación por parte de las agencias federales.

El hecho de que FortiSandbox forme parte de **Fortinet Security Fabric** incrementa el riesgo operativo, ya que un dispositivo comprometido puede alterar los resultados de análisis de archivos, distribuir veredictos erróneos a otros productos Fortinet y servir como punto de apoyo para comprometer la infraestructura empresarial.

Las ciertas vulnerabilidades ya habian sido alertadas semanas atras por Beaconlab, puede leer los detalles aquí.

Solución

Se recomienda a los administradores realizar las siguientes acciones:

- FortiSandbox 5.0.x 5.0.6 o superior.
- FortiSandbox 4.4.x 4.4.9 o superior.
- FortiSandbox Cloud 5.0.6 o superior.
- FortiSandbox PaaS 5.0.6 o superior.

Información adicional:

- BleepingComputer – CISA warns feds to patch exploited Fortinet FortiSandbox flaws by Sunday
- Fortinet PSIRT FG-IR-26-141
- BleepingComputer – Critical Fortinet FortiSandbox flaws now exploited in attacks
- Cybersecurity Dive – Critical Fortinet FortiSandbox vulnerabilities are under exploitation
- Arctic Wolf – CVE-2026-25089 Advisory