Boletín de alerta

Boletín Nro.: 04
Fecha de publicación: 14/01/2026
Tema: Alerta 2026-04 Vulnerabilidad de RCE en Fortinet FortiOS y FortiSwitchManager
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **FortiOS**
  - 6.4.0 hasta 6.4.16
  - 7.0.0 hasta 7.0.17
  - 7.2.0 hasta 7.2.11
  - 7.4.0 hasta 7.4.8
  - 7.6.0 hasta 7.6.3
- **FortiSASE**
  - 25.1.a.2
  - 25.2.b
- **FortiSwitchManager**
  - 7.0.0 hasta 7.0.5
  - 7.2.0 hasta 7.2.6

Descripción

Recientemente, Fortinet publicó un aviso de seguridad respecto a la **CVE-2025-25249**, una vulnerabilidad de **desbordamiento de heap (CWE-122)** que reside en el daemon **cw_acd** —parte del sistema de gestión/control de comunicaciones inalámbricas e infraestructura de FortiOS y FortiSwitchManager.

Esta falla permite que un **atacante remoto no autenticado** envíe **paquetes especialmente construidos** que desencadenan un desbordamiento de memoria en el heap. Como resultado, el atacante puede corromper el estado de memoria y, **en condiciones exitosas**, ejecutar **código o comandos arbitrarios** con privilegios del proceso afectado.

- **Naturaleza de la falla:** Heap-based buffer overflow
- **Vectores de ataque:** Paquetes de red especialmente construidos hacia la interfaz vulnerable
- **Condiciones de explotación:** Remota (no requiere autenticación)

El riesgo principal de esta vulnerabilidad radica en que podría permitir **ejecución remota de código (RCE)**, potencialmente comprometiendo el dispositivo o la infraestructura gestionada, lo cual impacta la **confidencialidad, integridad y disponibilidad** del sistema.

Solución y mitigación:

La mitigación principal recomendada por Fortinet consiste en **actualizar cuanto antes** los sistemas afectados:

1. **FortiOS:**
   - 7.6.x actualizar a **7.6.4 o superior**
   - 7.4.x actualizar a **7.4.9 o superior**
   - 7.2.x actualizar a **7.2.12 o superior**
   - 7.0.x actualizar a **7.0.18 o superior**
   - 6.4.x actualizar a **6.4.17 (o la próxima actualización segura)**
2. **FortiSASE**:
   - Actualizar a **25.2.c o superior** (Fortinet indica que esta versión ya contiene la corrección)
3. **FortiSwitchManager**:
   - Actualizar a las versiones **7.0.6 o superior** / **7.2.7 o superior** (si están disponibles según el canal de parches de Fortinet).

Mismos parches que se puede revisar en el siguiente enlace oficial:

FortiGuard Labs – Unauthenticated remote command injection

Recomendaciones adicionales:

- Realizar revisión de logs y telemetría de red para detectar paquetes anómalos con patrones inusuales.
- Aplicar controles de firewall o IPS/IDS que bloqueen tráfico no necesario hacia interfaces de gestión.
- Implementar segmentación de red para restringir el acceso a interfaces administrativas únicamente desde zonas de confianza.

Información adicional:

- https://www.fortiguard.com/psirt/FG-IR-25-084
- https://cybersecuritynews.com/fortios-and-fortiswitchmanager-vulnerability/
- https://www.cve.org/CVERecord?id=CVE-2025-25249