Boletín de alerta

Boletín Nro.:
Fecha de publicación: 28/05/2026
Tema: Alerta 2026-56 Vulnerabilidad crítica en Fortinet FortiClient EMS
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Fortinet FortiClient EMS 7.4.5
- Fortinet FortiClient EMS 7.4.6

Descripción

Fortinet publicó un parche de emergencia para corregir la vulnerabilidad crítica CVE-2026-35616, una falla de tipo Improper Access Control que afecta a FortiClient EMS (Enterprise Management Server). La vulnerabilidad permite a atacantes no autenticados ejecutar código o comandos arbitrarios mediante solicitudes especialmente manipuladas hacia la API expuesta del servidor EMS.

La vulnerabilidad fue clasificada con un puntaje CVSS v3.1 de 9.1 y se origina por un bypass de autenticación y autorización en la API de administración de FortiClient EMS.

Fortinet confirmó que la vulnerabilidad ya está siendo explotada activamente en entornos reales (in-the-wild exploitation), motivo por el cual CISA agregó el CVE al catálogo de Known Exploited Vulnerabilities (KEV).

Investigadores reportan intentos de explotación observados desde el 31 de marzo de 2026 contra sistemas expuestos a Internet.

La explotación exitosa podría permitir:

- Ejecución remota de código (RCE)
- Bypass de autenticación en API
- Ejecución arbitraria de comandos
- Compromiso del servidor EMS
- Alteración de políticas y configuraciones de endpoints
- Distribución maliciosa hacia endpoints administrados

FortiClient EMS es una plataforma centralizada utilizada para desplegar, configurar y monitorear agentes FortiClient dentro de entornos corporativos. Debido a esto, el impacto potencial puede extenderse a múltiples dispositivos administrados dentro de la organización.

Investigadores y firmas de seguridad consideran que esta vulnerabilidad representa una situación de respuesta de emergencia para organizaciones con instancias EMS expuestas a Internet.

Solución:

Se recomiendan la siguientes acciones de forma inmediata:

- Actualizar FortiClient EMS a la version 7.4.7 o superior.
- Restringir el acceso externo a la interfaz/API de EMS.

Información adicional:

- FortiGuard PSIRT Advisory FG-IR-26-099
- CVE-2026-35616 – CVE.org
- NVD – CVE-2026-35616
- CISA KEV Catalog
- The Hacker News – Fortinet Patches Actively Exploited CVE-2026-35616
- watchTowr Analysis