Nro. Alerta:	AL-2026-018	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	13-abr-2026	Vulnerabilidad crítica en FortiClient EMS permite ejecución remota de código (CVE-2026-35616)	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Ejecución remota de código (RCE) / Acceso no autenticado
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidad crítica en FortiClient EMS permite ejecución remota de código (CVE-2026-35616) - figura referencial

Fortinet informo mediante el lanzamiento de una actualización de emergencia para su producto FORTICLIENT EMS (Endpoint Management Server) sobre CVE-2026-35616, una vulnerabilidad critica de control de acceso inadecuado, la cual permite a un atacante no autenticado ejecute código o comandos no autorizados a través de solicitudes manipuladas en los sistemas.

III. INTRODUCCIÓN

Fortinet dispone de su propia arquitectura de ciberseguridad integrada denominada Fortinet Security Fabric, la cual implementa los principios de la malla de ciberseguridad (Cybersecurity Mesh Architecture, CSMA) mediante la integración de múltiples soluciones de seguridad en un ecosistema abierto e interoperable.
FortiClient EMS es más que una solución de protección de endpoints con un VPN Client incorporado, ya que integra endpoints dentro de Fortinet

Security Fabric, constituyendo una solución de administración de seguridad que facilita la gestión centralizada y escalable de estos múltiples dispositivos dentro de una red empresarial.

Además de las funciones tradicionales de protección de los endpoints, incorpora capacidades como antimalware, control de aplicaciones, detección de amenazas, gestión de dispositivos y la integración de funcionalidades de VPN que permiten a todos los dispositivos conectarse de forma segura a la red corporativa.

En este contexto, FortiClient EMS permite conectar, gestionar y proteger los endpoints (equipos con FortiClient), integrándolos dentro de dicha arquitectura unificada. Esto facilita la interconexión con dispositivos como FortiGate, así como con servidores, entornos en la nube y sistemas de análisis, permitiendo una operación de seguridad coordinada y centralizada en toda la infraestructura.

La explotación activa 0-day de CVE-2026-35616 fue detectada por primera vez el 31 de marzo del presente año por la plataforma de ciberseguridad en la nube WatchTowr, al hacer sujeto de ataque contra sus honeypots (sistema informático engañoso vulnerable)

El equipo FortiGuard de Fortinet la define como una falla de control de acceso inadecuada (CWE-284) en la API de FortiClient EMS versión 7.4.5 hasta 7.4.6, lo que permite que un atacante no autenticado pueda enviar solicitudes manipuladas para omitir las protecciones de autenticación y autorización por completo, logrando la ejecución de código en el servidor subyacente sin credenciales válidas o interacción del usuario.

Por todo esto, la vulnerabilidad crítica en este componente no afecta solo a un equipo aislado, sino que compromete la gestión de la seguridad del entorno empresarial, la visibilidad sobre los dispositivos y la capacidad de respuesta de la organización. Esta relevancia aumenta especialmente cuando el sistema está expuesto o accesible desde redes no confiables.

IV. VECTOR DE ATAQUE

Esta vulnerabilidad posee una severidad CRITICAL con una puntación CVSSv3 de 9.8 tipo /AV:N NETWORK

V. IMPACTO

Los productos y versiones afectados son los siguientes:

Producto	Versión
FORTICLIENT EMS	7.4.5
FORTICLIENT EMS	7.4.6

Tabla 1.- Los Productos y Versiones Afectadas - Vulnerabilidad crítica en FortiClient EMS permite ejecución remota de código (CVE-2026-35616)

VI. INDICADORES DE COMPROMISO

A la fecha Fortinet no ha publicado indicadores de compromiso. La detección actualmente se basa en la revisión de registro y la auditoría de configuración en lugar de la coincidencia definitiva del IOC.

VII. RECOMENDACIONES:

- Aplicar los hotfixes publicados por Fortinet para FortiClient EMS versiones 7.4.5 y 7.4.6.
- Verificar la versión instalada y confirmar que los parches se hayan aplicado correctamente siguiendo la guía oficial.
- Restringir el acceso a FortiClient EMS desde internet, limitándolo solo a direcciones IP confiables.
- Limitar la exposición de la consola de administración, reforzar el control de acceso y monitorizar cualquier actividad anómala relacionada con solicitudes sospechosas o cambios no autorizados.
- Implementar reglas de firewall estrictas para reducir la superficie de ataque del servidor EMS.
- Monitorear logs y eventos de seguridad en busca de actividad sospechosa o indicadores de compromiso.
- Actualizar a FortiClient EMS 7.4.7 tan pronto esté disponible para contar con la corrección integrada.
- Desactivar servicios y APIs no utilizados para evitar abusos por parte de atacantes.
- Realizar escaneos de vulnerabilidades periódicos para detectar otras fallas explotables, como inyección SQL.
- Establecer un plan de respuesta a incidentes, incluyendo copias de seguridad y procedimientos de aislamiento.

- Capacitar al equipo de TI y seguridad sobre la amenaza y la importancia de aplicar actualizaciones críticas de forma oportuna

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

FORTINET (2026). FortiClient EMS Vulnerability Advisory (FG-IR-26-099). https://fortiguard.fortinet.com/psirt/FG-IR-26-099

NVD - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2026). CVE-2026-35616. https://nvd.nist.gov/vuln/detail/CVE-2026-35616

LINKEDIN (2026). Critical Fortinet FortiClient EMS Vulnerability. https://www.linkedin.com/pulse/critical-fortinet-forticlient-ems-vulnerability-xqwre

CIBERSAFETY (2026). CVE-2026-35616 en FortiClient EMS de Fortinet. https://cibersafety.com/cve-2026-35616-forticlient-ems-fortinet/

WATCHTOWR (2026). Fortinet FortiClient EMS Zero-Day CVE-2026-35616 Active Exploitation Underway. https://watchtowr.com/resources/fortinet-forticlient-ems-zero-day-cve-2026-35616-active-exploitation-underway/

CYBERSECURITY NEWS (2026). CISA warns about Fortinet vulnerability CVE-2026-35616. https://cybersecuritynews.com/cisa-warns-fortinet-vulnerability/