Boletín de alerta

Boletín Nro.: 34
Fecha de publicación: 04/04/2026
Tema: Alerta 2026-34 Omisión de Autenticación y Autorización de API en FortiClientEMS
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Afecta a FortiClientEMS 7.4: 7.4.5 y 7.4.6

Descripción

Se ha reportado una vulnerabilidad de control de acceso inadecuado [CWE-284] en FortiClient EMS puede permitir que un atacante no autenticado ejecute código o comandos no autorizados mediante solicitudes manipuladas. Se lo a identificado como CVE-2026-35616 con un score de 9.1 (crítico).

Fortinet ha observado que esta vulnerabilidad se está explotando en la práctica e insta a los clientes vulnerables a instalar la actualización para FortiClient EMS 7.4.5 y 7.4.6. Esta vulnerabilidad puede ser utilizada por los atacantes entre otras cosas para escalar privilegios en los dispositivos.

Solución:

El fabricante a preparado una serie de notas para aplicar el hotfix en las versiones afectadas:
• FortiClient EMS 7.4.5: https://docs.fortinet.com/document/forticlient/7.4.5/ems-release-notes/832484
• FortiClient EMS 7.4.6: https://docs.fortinet.com/document/forticlient/7.4.6/ems-release-notes/832484

Información adicional:

- https://www.fortiguard.com/psirt/FG-IR-26-099
- https://nvd.nist.gov/vuln/detail/CVE-2026-35616