ALERTA

Vulnerabilidad Crítica FortiManager (CVE-2024-47575)

[COLCERT AL-2510-053]

TPL CLEAR

Se ha detectado una vulnerabilidad crítica (CVE-2024-47575) en Fortinet, que afecta a las plataformas FortiManager y FortiManager Cloud. A esta se le ha asignado una puntuación CVSS v3 de 9,8, la falla permite a atacantes remotos no autenticados ejecutar código o comandos arbitrarios mediante el envío de solicitudes especialmente diseñadas, lo que representa un riesgo significativo para la seguridad de la red

La vulnerabilidad surge de una autenticación insuficiente para funciones de administración críticas dentro del servicio fgfmd, que facilita la comunicación entre los dispositivos FortiManager y FortiGate.

ANÁLISIS

Si no se realiza la actualización para corregir la vulnerabilidad, las entidades/organizaciones se exponen a riesgos como la ejecución remota de código, lo que podría permitir a los atacantes tomar control total del dispositivo afectado. Además, los atacantes lograrían acceder a datos sensibles, moverse lateralmente dentro de la red comprometiendo otros sistemas y servicios, y causar interrupciones operativas significativas. Dado que esta vulnerabilidad tiene una puntuación CVSS de 9.8, es extremadamente crítica y debe ser gestionada de manera urgente para evitar estos riesgos.

Acciones inmediatas:

Es critico aplicar los parches y mitigaciones recomendadas por Fortinet, actualizando la herramienta FortiManager de gestión de dispositivos de red y seguridad FortiGate a una versión corregida. Para validar esta información y obtener más detalles, consultar la siguiente URL: https://fortiguard.fortinet.com/psirt/FG-IR-24-423

NIVEL DE RIESGO

ALTO

FUENTES:

https://www.cisa.gov/news-events/alerts/2024/10/23/cisa-adds-one-known-exploited-vulnerability-catalog
https://nvd.nist.gov/vuln/detail/CVE-2024-47575
https://fortiguard.fortinet.com/psirt/FG-IR-24-423
https://censys.com/es/cve-2024-47575/

COLCERT