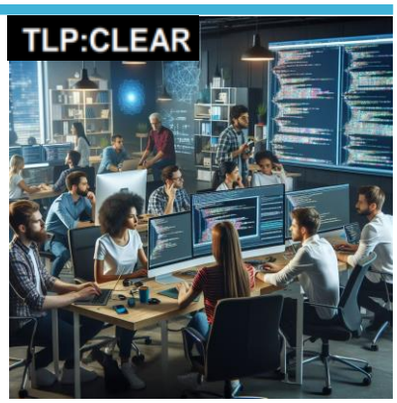
TIC

ALERTA

Múltiples vulnerabilidades en productos Fortinet

COLCERT AL-2012-061



Fortinet ha emitido avisos de seguridad para abordar varias vulnerabilidades críticas en sus productos, incluyendo FortiWLM. La más destacada es CVE-2023-34990, una vulnerabilidad de recorrido de ruta relativa en FortiWLM, que podría permitir a los atacantes remotos no autenticados, acceder en archivos confidenciales y potencialmente ejecutar código arbitrario.

Las siguientes versiones están afectadas: *8.6.0 hasta 8.6.5; 8.5.0 hasta 8.5.4.*

Esta vulnerabilidad tiene un puntaje CVSS de 9.6, lo que indica un riesgo extremadamente alto para los sistemas afectados.

ELEMENTOS DE INTELIGENCIA DISPONIBLES

La combinación de CVE-2023-34990 con otras vulnerabilidades, como CVE-2023-48782 (una falla de inyección de comandos), podría permitir a un atacante obtener acceso a los sistemas con privilegios de root, lo que podría conllevar a poder realizar cualquier acción, desde robar datos hasta tomar el control completo del sistema. En esta línea, la limitación incorrecta de una ruta a un directorio restringido en FortiWLM de Fortinet.

RECOMENDACIONES

- ❑ Aplicar los parches de seguridad lo antes posible. (Ver fuentes) [1]
- ❑ Realizar una revisión exhaustiva de la configuración de los dispositivos Fortinet.
- ❑ Implementar medidas de seguridad adicionales como: la segmentación de redes, el uso de firewalls y la autenticación multifactor.
- ❑ Mantener un programa de gestión de parches actualizado.

IMPACTO PARA COLOMBIA Y LA REGIÓN

Las vulnerabilidades conocidas en dispositivos de red como FortiWLM representan un riesgo significativo para la seguridad de las organizaciones, ya que las amenazas pueden explotar activamente estas debilidades para obtener acceso a sistemas y redes. El impacto a Colombia se da por los dispositivos que pueden estar expuestos, los atacantes podrían acceder a información sensible de organizaciones colombianas, además, existe riesgo de comprometer sistemas gubernamentales si están usando FortiWLM no actualizado. Las empresas que manejan datos personales podrían enfrentar problemas de cumplimiento. Así pues, es fundamental que las organizaciones tomen medidas proactivas para protegerse, como mantener sus sistemas actualizados y siguiendo las mejores prácticas de seguridad.

NIVEL DE RIESGO

Alto

FUENTES:

[1] https://www.fortiguard.com/psirt/FG-IR-23-144
[2] https://securelist.com/patched-forticlient-ems-vulnerability-exploited-in-the-wild/115046/
[3] https://www.securityweek.com/fortinet-patches-critical-fortiwlm-vulnerability/

COLCERT