BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-72
Fecha de publicación: 27/12/2024
Tema: Vulnerabilidades Crítica en FortiWLM y FortiManager
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

CVE-2023-34990:

- FortiWLM 8.6, 8.6.0 a 8.6.5
- FortiWLM 8.5, 8.5.0 a 8.5.4

CVE-2024-48782:

- FortiWLM 8.6, 8.6.0 a 8.6.5

CVE-2024-48889:

- FortiManager 7.6.0 (corregido en 7.6.1 o posterior)
- Versiones de FortiManager 7.4.0 a 7.4.4 (corregidas en 7.4.5 o posteriores)
- Versiones 7.4.1 a 7.4.4 de FortiManager Cloud (corregidas en 7.4.5 o posteriores)
- Versiones 7.2.3 a 7.2.7 de FortiManager (corregidas en 7.2.8 o superior)
- Versiones 7.2.1 a 7.2.7 de FortiManager Cloud (corregidas en 7.2.8 o posteriores)
- Versiones de FortiManager 7.0.5 a 7.0.12 (corregidas en 7.0.13 o posteriores)
- Versiones 7.0.1 a 7.0.12 de FortiManager Cloud (corregidas en 7.0.13 o posteriores)
- Versiones de FortiManager 6.4.10 a 6.4.14 (corregidas en 6.4.15 o posterior)

Descripción

Se ha publicado varias vulnerabilidades para productos Fortinet que pueden combinarce y volverse críticas. Ambas vulnerabilidades afectan al software Wireless LAN Manager (FortiWLM) de Fortinet, la primera vulnerabilidad de tipo path-traversal denominada CVE-2023-34990 con puntuación CVSSv3 9.6 con crititicidad crítica. Y la otra vulnerabilidad de tipo de inyección de comandos, con criticidad Alta y denominada como CVE-2023-48782 con puntuación CVSSv3 8.6, que pueden ser combinadas y podrian generar un RCE.

Una explotación exitosa de CVE-2023-34990 podría permitir al actor de amenazas leer archivos de registro de FortiWLM y obtener el ID de sesión de un usuario y su inicio de sesión, lo que le permitiría explotar también puntos finales autenticados. Los atacantes podrían aprovechar el hecho de que los ID de las sesiones web son estáticos entre las sesiones de usuario para secuestrarlos y obtener permisos administrativos en el dispositivo.

Un atacante también podría combinar CVE-2023-34990 con CVE-2023-48782 una falla de inyección de comandos autenticados que también se ha corregido en FortiWLM 8.6.6, para obtener la ejecución remota de código en el contexto de la raíz.

Ademas, el equipo de Fortinet ha corregido otra vulnerabilidad que afecta al producto FortiManager, la misma denominada como CVE-2024-48889 con puntuación CVSS: 7.2 de tipo inyección de comandos del sistema operativo. Fortinet también señaló que varios modelos más antiguos, 1000E, 1000F, 2000E, 3000E, 3000F, 3000G, 3500E, 3500F, 3500G, 3700F, 3700G y 3900E, están afectados por CVE-2024-48889 siempre que el "fmg-status" esté habilitado.

Recomendamos aplicar medidas de seguridad sobre estos productos, especialmente al tratarse de productos de seguridad utilizados comumente en organizaciones, los mismos pueden utilizarse como vector de entrada por los atacantes.

Solución

El proveedor a publicado parches de seguridad para los productos FortiWLM y FortiManager, puede dirigirse a los enlace de actualización proveidos por el fabricante:

- FortiWLM
  - Version 8.6 https://docs.fortinet.com/product/fortiwlm/8.6
  - Version 8.5 https://docs.fortinet.com/product/fortiwlm/8.5
- FortiManager
  - Versiones Varias https://docs.fortinet.com/product/fortimanager/7.6

Información adicional:

- https://www.fortiguard.com/psirt/FG-IR-23-144
- https://www.cve.org/CVERecord?id=CVE-2023-34990
- https://thehackernews.com/2024/12/fortinet-warns-of-critical-fortiwlm.html

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com