BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-14
Fecha de publicación: 14/02/2025
Tema: Vulnerabilidad de Escalación de Privilegios en FortiOS de Fortinet.
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Las vulnerabilidades afectan a las siguientes versiones de FortiOS:

- 7.6.0, 7.4.0 a 7.4.4, 7.2.0 a 7.2.9, 7.0.0 a 7.0.15 y todas las versiones de 6.4.

Descripción

Se ha reportado una vulnerabilidad alta de tipo escalación de privilegios que afecta al sistema FortiOS utilizado por varios productos de la empresa Fortinet, la vulnerabilidad ha sido identificada como CVE-2024-40591 con un puntaje de CVSSv3 8.0.

La vulnerabilidad se origina por una administración incorrecta de privilegios, específicamente una asignación incorrecta de privilegios.

La vulnerabilidad puede explotarse si un actor malintencionado obtiene el control de un dispositivo FortiGate de nivel superior. Al conectar un FortiGate de destino a este dispositivo de nivel superior comprometido, el atacante podría aprovechar la asignación incorrecta de privilegios para obtener acceso de superadministrador. Este nivel de acceso otorga un amplio control sobre el sistema afectado, lo que puede dar lugar a importantes brechas de seguridad.

En este tipo de situaciones, es posible que un agente de amenazas obtenga privilegios de superadministrador en un sistema de seguridad diseñado para proteger a las empresas. Este nivel de acceso puede permitir a los atacantes obtener el control total de la infraestructura de seguridad, lo que puede provocar violaciones generalizadas de la red, exfiltración de datos y otras actividades maliciosas.

Esta vulnerabilidad puede ser especialmente crítica si se combina con otras técnicas post explotación durante el compromiso de una organización.

Solución

El proveedor Fortinet hay proveído parches de seguridad que soluciones, recomendamos planear una actualización lo más pronto posible.

Puede encontrar el enlace del reporte de seguridad a continuación:
https://www.fortiguard.com/psirt/FG-IR-24-302

Version	Afectado	Solución
FortiOS 7.6	7.6.0	Actualizar to 7.6.1 o superior
FortiOS 7.4	7.4.0 hasta 7.4.4	Actualizar to 7.4.5 o superior
FortiOS 7.2	7.2.0 hasta 7.2.9	Actualizar to 7.2.10 o superior
FortiOS 7.0	7.0.0 hasta 7.0.15	Actualizar to 7.0.16 o superior
FortiOS 6.4	6.4 toda sus versiones	Migrar a una version estable superior

En el siguiente enlace puede encontrar una herramienta que le puede ayudar en la actualización de sus dispositivos.

https://docs.fortinet.com/upgrade-tool/fortigate

Información adicional:

- https://www.fortiguard.com/psirt/FG-IR-24-302
- https://github.com/advisories/GHSA-hmpg-p67j-959p
- https://hackread.com/fortios-vulnerability-super-admin-privilege-escalation/

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com