BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-12
Fecha de publicación: 28/05/2024
Tema: Publicación de exploit para Fortinet.
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- FortiClient FortiSIEM.
  - Version:
  - 7.1.0-7.1.1
  - 7.0.0-7.0.2
  - 6.7.0-6.7.8
  - 6.6.0-6.6.3
  - 6.5.0-6.5.2
  - 6.4.0-6.4.2

Descripción:

El martes 28 de mayo, un grupo de investigadores de ciberseguridad han publicado exploit de la vulnerabilidad denominada como CVE-2024-23109, con severidad crítica y puntuación CVSS de 9.8, que afecta Fortinet FortiSIEM.

La vulnerabilidad reside en una debilidad de sanitización de comando SQL que permite la inyección de comandos a nivel de sistema operativo como el usuario root, esto puede ser logrado a través de la red y sin interacción de algún tercero.

Es importante mencionar que esta vulnerabilidad fue publicada en el mes de febrero, sin embargo, la publicación del exploit, eleva mucho el riesgo de explotación en caso de contar con alguna de las versiones vulnerables del producto; se recomienda encarecidamente la pronta actualización a alguna versión segura.

Además, hay que tener en cuenta que las vulnerabilidades en productos de Fortinet son frecuentemente explotadas, llevando a ataques de ransomware o ciberespionaje en redes empresariales o gubernamentales.

Impacto

Un actor malintencionado que tenga la posibilidad de alcanzar a través de la red el dispositivo Fortinet FortiSIEM, tiene la capacidad de ejecutar el exploit y ejecutar comandos a nivel de sistema operativo con usuario privilegiado, que podría desencadenarse en una catástrofe, pues podría hacerse con el dispositivo y extender el ataque por toda la red.

Solución

Aplicar el parche oficial publicado por Fortinet.

Información adicional:

- https://www.bleepingcomputer.com/news/security/exploit-released-for-fortinet-rce-bug-used-in-attacks-patch-now/
- https://www.bleepingcomputer.com/news/security/exploit-released-for-fortinet-rce-bug-used-in-attacks-patch-now/
- https://nvd.nist.gov/vuln/detail/CVE-2024-23108

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com