Boletín de alerta

Boletín Nro.:
Fecha de publicación: 13/08/2025
Tema: Alerta 2025-68 Vulnerabiliad en FortiSIEM
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

FortiSIEM

- FortiSIEM 6.1, 6.2, 6.3, 6.4, 6.5, 6.6
- FortiSIEM 6.7.0 – 6.7.9
- FortiSIEM 7.0.0 – 7.0.3
- FortiSIEM 7.1.0 – 7.1.7
- FortiSIEM 7.2.0 – 7.2.5
- FortiSIEM 7.3.0 – 7.3.1

Descripción

Se ha reportado la vulnerabilidad **CVE-2025-25256** con **CVSS 9.8** en FortiSIEM:

La vulnerabilidad se deriva de la neutralización incorrecta de elementos especiales utilizados en comandos del sistema operativo, clasificados como CWE-78 (inyección de comandos del sistema operativo).

Esta falla de seguridad permite a atacantes no autenticados ejecutar código o comandos arbitrarios mediante solicitudes CLI especialmente diseñadas en los sistemas FortiSIEM afectados. Por lo cual se pueden explotar sistemas vulnerables a través de internet cuando está expuesto, sin necesidad de acceso

La naturaleza remota del vector de ataque lo hace particularmente peligroso, ya que los actores de amenazas pueden explotar sistemas vulnerables a través de internet sin necesidad de acceso previo ni credenciales.

Una explotación exitosa de esta vulnerabilidad podría otorgar a los atacantes control total sobre la infraestructura SIEM, lo que podría permitirles manipular registros de seguridad, desactivar las funciones de monitorización o utilizar el sistema comprometido como punto de partida para el movimiento lateral dentro de la red.

Mitigación:

Se recomienda migrar a las versiones 6.7.10, 7.0.4, 7.1.7, 7.2.5, 7.3.1 o 7.4. Como medida adicional monitorear o limitar el acceso al puerto 7900

Información adicional:

- https://thehackernews.com/2025/08/fortinet-warns-about-fortisiem.html
- https://www.helpnetsecurity.com/2025/08/13/fortinet-warns-about-fortisiem-vulnerability-with-in-the-wild-exploit-code-cve-2025-25256/
- https://www.fortiguard.com/psirt/FG-IR-25-152

  https://www.cybersecurity-help.cz/vulnerabilities/113969