ALERTA

Afectación a Productos SIEM Fortinet

[COLCERT AL-0529-028]

TLP:CLEAR

”POC: Riesgo asociado a Explotación de Vulnerabilidad en productos Fortinet”

El equipo de ataque de Horizon3 ha publicado un exploit de prueba de concepto (PoC), para una vulnerabilidad de ejecución remota de código en la solución SIEM de Fortinet, conocida como: **CVE-2024-23108.**

Elementos de la POC

- **Vulnerabilidades:** CVE-2024-23108, CVE-2024-23109.
- **Impacto:** Ejecución remota de código como root.
- **Productos afectados:** FortiSIEM.
- **Exploit:** PoC público disponible.
- **Vector de ataque:** Solicitudes API no autenticadas.

Impacto:

- **Impacto potencial:** Toma de control total del dispositivo FortiSIEM.
- Robo de datos confidenciales – Confidencialidad.
- Interrupción del servicio – Disponibilidad.
- Instalación de malware - Integridad

Recomendación para realizar la PoC:

Aplicar parches de inmediato: CVE-2024-23108 y CVE-2024-23109
Implementar medidas de seguridad en profundidad: Fortalecer la seguridad general con firewalls, antivirus y políticas de gestion de vulnerabilidades.
Monitorear la actividad de la red: Identificar actividades de precursores e indicadores inusuales que puedan indicar intentos de explotación.

Es importante realizar una adecuada gestión de vulnerabilidades, para evitar riesgos de explotación, que afecten la continuidad de las operaciones.

NIVEL DE RIESGO

ALTO

FUENTES:

https://securityaffairs.com/163797/hacking/fortinet-siem-critical-rce-poc.html
https://github.com/horizon3ai/CVE-2024-23108
https://nvd.nist.gov/vuln/detail/CVE-2024-23108 https://www.cve.org/CVERecord?id=CVE-2023-38709
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/e3bf4b6d-2b27-11ee-8e6d-fa163e15d75b/FortiCentral-7.0.1-User-Guide.pdf