Alerta de seguridad cibernética	9VSA23-00936-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	21 de noviembre de 2023
Última revisión	21 de noviembre de 2023

NOTIFICACIÓN: La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de una nueva vulnerabilidad crítica que afecta a FortiSIEM de Fortinet.

Vulnerabilidades

CVE-2023-36553

Impacto

Vulnerabilidades de riesgo crítico:
CVE-2023-36553: Vulnerabilidad de inyección de comandos en el servidor de informes de FortiSIEM.
CVSS: 9.3.

Mitigación
Instalar las respectivas actualizaciones entregadas por el proveedor (https://support.fortinet.com/):
FortiSIEM versión 7.1.0 o superior
FortiSIEM versión 7.0.1 o superior
FortiSIEM versión 6.7.6 o superior
FortiSIEM versión 6.6.4 o superior
FortiSIEM versión 6.5.2 o superior
FortiSIEM versión 6.4.3 o superior

Productos afectados
FortiSIEM 5.4 en todas sus versiones
FortiSIEM 5.3 en todas sus versiones
FortiSIEM 5.2 en todas sus versiones
FortiSIEM 5.1 en todas sus versiones
FortiSIEM 5.0 en todas sus versiones
FortiSIEM 4.10 en todas sus versiones
FortiSIEM 4.9 en todas sus versiones

FortiSIEM 4.7 en todas sus versiones

Enlaces

https://www.fortiguard.com/psirt/FG-IR-23-135
https://nvd.nist.gov/vuln/detail/CVE-2023-36553

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.29 15:13:50 -03'00'