Alerta de seguridad cibernética	9VSA21-00471-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de julio de 2021
Última revisión	20 de julio de 2021

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 equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre una nueva vulnerabilidad que afecta a FortiAnalyzer y FortiManager de Fortinet.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidad

CVE-2021-32589

Impactos

La vulnerabilidad corresponde a un error de uso de memoria después de ser liberada, que permite a un atacante remoto no autenticado ejecutar código no autorizado como root, a través del envío de una solicitud especialmente diseñada al puerto fgfm del aparato objetivo.

Productos Afectados

FortiManager 5.6.10 y anteriores.
FortiManager 6.0.10 y anteriores.
FortiManager 6.2.7 y anteriores.
FortiManager 6.4.5 y anteriores.
FortiManager 7.0.0.
FortiManager 5.4.x.
FortiAnalyzer 5.6.10 y anteriores.
FortiAnalyzer 6.0.10 y anteriores.
FortiAnalyzer 6.2.7 y anteriores.

FortiAnalyzer 6.4.5 y anteriores.
FortiAnalyzer 7.0.0.

Mitigación

Instalar las respectivas actualizaciones del proveedor.

Enlaces

https://www.fortiguard.com/psirt/FG-IR-21-067
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2021-32589

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.20 10:26:22 -04'00'