Alerta de seguridad cibernética	9VSA23-00794-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	22 de febrero de 2023
Última revisión	22 de febrero 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 Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre una vulnerabilidad crítica en FortiOS y FortiAuthenticator.

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

Vulnerabilidad

CVE-2022-22302

Impacto

Esta vulnerabilidad puede permitir que una parte local no autorizada recupere las claves privadas de Fortinet utilizadas para establecer una comunicación segura con los servicios Apple Push Notification y Google Cloud Messaging, mediante el acceso a los archivos en el sistema de archivos.

Productos afectados

FortiOS versión 6.4.0 a 6.4.1
FortiOS versión 6.2.0 a 6.2.9
FortiOS versión 6.0.0 a 6.0.13
FortiAuthenticator versión 6.1.0
FortiAuthenticator versión 6.0.0 a 6.0.4
FortiAuthenticator 5.5 todas las versiones

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.fortiguard.com/psirt/FG-IR-20-014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22302

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.22 13:02:36 -03'00'