Alerta de seguridad cibernética	9VSA23-00799-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2023
Última revisión	3 de marzo 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 múltiples vulnerabilidades en productos Fortinet.

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

Vulnerabilidad

CVE-2023-23781
CVE-2023-23780
CVE-2023-23779

Impacto

CVE-2023-23781: Esta vulnerabilidad puede permitir a un atacante autenticado lograr la ejecución de código arbitrario a través de archivos XML específicamente diseñados.

CVE-2023-23780: Un desbordamiento de búfer basado en pila en las versiones Fortinet afectadas permite una escalada de privilegios a través de peticiones HTTP específicamente diseñadas.

CVE-2023-23779: La nutralización incorrecta múltiple de elementos especiales utilizados en un comando OS ('OS Command Injection') en las versiones FortiWeb afectadas puede permitir a un atacante autenticado ejecutar código o comandos no autorizados a través de parámetros manipulados de peticiones HTTP.

Productos afectados

FortiWeb versión 7.0.0 a 7.0.1
FortiWeb versión 6.3.0 a 6.3.19
FortiWeb 6.4 todas las versiones

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://s2grupo.es/multiples-vulnerabilidades-en-productos-de-fortinet/?utm_content=239987244&utm_medium=social&utm_source=twitter&hss_channel=tw-45396268
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23781
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23780
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23779