Alerta de seguridad cibernética	9VSA23-00903-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2023
Última revisión	20 de septiembre 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 nuevas vulnerabilidades de severidad alta, que fueron parchadas y que afectan a distintos productos de Fortinet.

Vulnerabilidades

CVE-2023-29183
CVE-2023-34984

Impacto

Vulnerabilidades de riesgo alto

CVE-2023-29183: Vulnerabilidad que permite la ejecución de código o comandos no autorizados. CVSS: 7.3.

CVE-2023-34984: Vulnerabilidad que permite la ejecución de código o comandos no autorizados. CVSS: 7.1.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

CVE-2023-34984: FortiWeb 6.3.6 a 7.2.1.

CVE-2023-29183: FortiProxy 7.0.0 a 7.2.4.
FortiOS 6.2.0 a 7.2.4.

Enlaces

https://www.fortiguard.com/psirt/FG-IR-23-106
https://www.fortiguard.com/psirt/FG-IR-23-068

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29183

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.20 16:43:20 -03'00'