Alerta de seguridad cibernética	9VSA23-00847-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	13 de junio de 2023
Última revisión	13 de junio 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 cinco vulnerabilidades, incluyendo una vulnerabilidad crítica, parchadas por Fortinet para su producto FortiGate SSL. Esta vulnerabilidad crítica ya había sido tratada por el CSIRT en el documento https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00846-01/. La recomendación sigue siendo parchar cuanto antes con la actualización que haga disponible Fortinet.

Vulnerabilidades

CVE-2023-27997
CVE-2023-22640
CVE-2023-29179
CVE-2023-29180
CVE-2023-29181
CVE-2023-22641

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-27997: Vulnerabilidad que afecta todos las VPN SSL y que puede ser explotada para lograr ejecución remota de código sin autenticación. CVSS 9.2.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

FortiGate SSL. Parche presente en la más reciente actualización de firmware.

Enlaces

https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27997

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29180

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22640
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29181
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29179
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22641

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.13 14:20:16 -04'00'