Alerta de seguridad cibernética	9VSA22-00745-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de noviembre de 2022
Última revisión	15 de noviembre de 2022

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, CSIRT de Gobierno, comparte información entregada por Citrix sobre vulnerabilidades en algunos de sus productos.

Vulnerabilidades

CVE-2022-27510 CVE-2022-27513 CVE-2022-27516

Impacto

Vulnerabilidades de mayor riesgo

CVE-2022-27510: Bypass de autenticación que permite acceso no autorizado a las capacidades de usuario en Gateway. Para ser vulnerable, el dispositivo objetivo debe estar configurado como Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy).

Productos afectados

Citrix Gateway
Citrix ADC

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27510
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27513
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27516

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.11.15 15:16:10 -03'00'

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob