

Alerta de seguridad cibernética	9VSA21-00507-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de octubre de 2021
Última revisión	15 de octubre de 2021

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 equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre vulnerabilidades recientemente conocidas en Google Chrome.

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

Vulnerabilidades

CVE-2021-37977
CVE-2021-37978
CVE-2021-37979
CVE-2021-37980

Impactos

Vulnerabilidades de alto impacto.

CVE-2021-37977: Esta vulnerabilidad existe debido a un error de memoria luego de ser liberada dentro del componente Garbage Collection en Google Chrome, y puede permitir a un atacante remoto ejecutar código arbitrario en el sistema objetivo.

CVE-2021-37978: Esta vulnerabilidad existe debido a un error de límites de la memoria al procesar contenido HTML no confiable en Blink. Si un atacante remoto detona un desborde de buffer podría ejecutar código arbitrario en el sistema objetivo.

CVE-2021-37979: Esta vulnerabilidad existe debido a un error de límites de la memoria al procesar contenido HTML no confiable en WebRTC. Si un atacante remoto detona un desborde de buffer podría ejecutar código arbitrario en el sistema objetivo.

Productos Afectados

Google Chrome: 7.0.517.41 a 94.0.4606.71.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37977>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37978>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37979>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37980>