

Alerta de seguridad cibernética	9VSA21-00457-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2021
Última revisión	17 de junio 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 críticas que afectan a Google Chrome. La vulnerabilidad CVE-2021-30554 ya está siendo explotada.

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

Vulnerabilidades

CVE-2021-30554 CVE-2021-30556
CVE-2021-30555 CVE-2021-30557

Impactos

La siguiente vulnerabilidad es considerada crítica.

CVE-2021-30554: Vulnerabilidad que existe debido a un error de uso de memoria después de ser liberada dentro del componente WebGL en Google Chrome. Un atacante remoto puede crear una página web, convencer a la víctima para que haga click en él, y así detonar el error y ejecutar código en el sistema objetivo, pudiendo llegar a comprometerlo.

Las siguientes vulnerabilidades son consideradas como de riesgo alto.

CVE-2021-30553: Vulnerabilidad que existe debido a un error de uso de memoria después de ser liberada dentro del componente Sharing en Google Chrome. Un atacante remoto puede crear una

página web, convencer a la víctima para que haga click en él, y así detonar el error y ejecutar código en el sistema objetivo, pudiendo llegar a comprometerlo.

CVE-2021-30556: Vulnerabilidad que existe debido a un error de uso de memoria después de ser liberada dentro del componente WebAudio en Google Chrome. Un atacante remoto puede crear una página web, convencer a la víctima para que haga click en él, y así detonar el error y ejecutar código en el sistema objetivo, pudiendo llegar a comprometerlo.

CVE-2021-30557: Vulnerabilidad que existe debido a un error de uso de memoria después de ser liberada dentro del componente TabGroups en Google Chrome. Un atacante remoto puede crear una página web, convencer a la víctima para que haga click en él, y así detonar el error y ejecutar código en el sistema objetivo, pudiendo llegar a comprometerlo.

Productos Afectados

Google Chrome: 89.0.4389.72 a 91.0.4472.101.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30554>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30555>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30556>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30557>