Alerta de seguridad cibernética	9VSA21-00523-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de noviembre de 2021
Última revisión	16 de noviembre 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 afecta a actualizaciones.

Resumen

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

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

Vulnerabilidades

CVE-2021-38007
CVE-2021-38015
CVE-2021-38022
CVE-2021-38021
CVE-2021-38020
CVE-2021-38019
CVE-2021-38018
CVE-2021-38017
CVE-2021-38016
CVE-2021-38014
CVE-2021-38008
CVE-2021-38013
CVE-2021-38012
CVE-2021-38011
CVE-2021-38010
CVE-2021-38005
CVE-2021-38006
CVE-2021-38009

Impactos

Vulnerabilidades de riesgo alto:

CVE-2021-38007: Permite a un atacante remoto ejecutar código arbitrario en el objetivo, debido a un error de confusión de tipo de archivo en el componente V8 de Google Chrome.

CVE-2021-38015: Permite a un atacante remoto conseguir acceso a información sensible, debido a una implementación incorrecta en input en Google Chrome.

CVE-2021-38021: Permite a un atacante remoto conseguir acceso a información sensible, debido a una implementación incorrecta en referrer de Google Chrome.

CVE-2021-38018: Permite a un atacante remoto conseguir acceso a información sensible, debido a una implementación incorrecta en navigation de Google Chrome.

CVE-2021-38008: Permite a un atacante remoto comprometer un sistema vulnerable, debido a un error de uso de memoria después de ser liberada en el componente media de Google Chrome.

CVE-2021-38011: Permite a un atacante remoto comprometer un sistema vulnerable, debido a un error de uso de memoria después de ser liberada en el componente storage foundation de Google Chrome.

CVE-2021-38005: Permite a un atacante remoto comprometer un sistema vulnerable, debido a un error de uso de memoria después de ser liberada en el componente loader de Google Chrome.

CVE-2021-38006: Permite a un atacante remoto comprometer un sistema vulnerable, debido a un error de uso de memoria después de ser liberada en el componente storage foundation de Google Chrome.

Productos Afectados

Google Chrome: 7.0.517.41 a 95.0.4638.69

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38018

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38009

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.11.16 16:00:10 -03'00'