Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00529-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de diciembre de 2021
Última revisión	7 de diciembre 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-2021-4062
CVE-2021-4068
CVE-2021-4067
CVE-2021-4066
CVE-2021-4065
CVE-2021-4064
CVE-2021-4063
CVE-2021-4061
CVE-2021-4052
CVE-2021-4059
CVE-2021-4058
CVE-2021-4057
CVE-2021-4056
CVE-2021-4055
CVE-2021-4054
CVE-2021-4053

Impactos

Vulnerabilidades graves

CVE-2021-4062: Esta vulnerabilidad permite a un atacante remoto comprometer los sistemas afectados. La vulnerabilidad existe debido a un error de límites de la memoria al procesar HTML no confiable en BFCache.

CVE-2021-4067: Esta vulnerabilidad permite a un atacante remoto comprometer los sistemas afectados. La vulnerabilidad existe debido a un error de memoria luego de ser liberada dentro de componente de administración de ventanas en Google Chrome.

CVE-2021-4066: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. Existe debido a un integer underflow.

CVE-2021-4065: Esta vulnerabilidad permite a un atacante remoto comprometer los sistemas afectados. La vulnerabilidad existe debido a un error de memoria luego de ser liberada dentro de componente autofill en Google Chrome

CVE-2021-4064: Esta vulnerabilidad permite a un atacante remoto comprometer los sistemas afectados. La vulnerabilidad existe debido a un error de memoria luego de ser liberada dentro de componente de captura de pantalla en Google Chrome.

CVE-2021-4063: Esta vulnerabilidad permite a un atacante remoto comprometer los sistemas afectados. La vulnerabilidad existe debido a un error de memoria luego de ser liberada dentro del componente developer tools en Google Chrome.

CVE-2021-4061: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. Existe debido a un error de confusión de tipo de archivo dentro del componente V8 de Google Chrome.

CVE-2021-4052: Esta vulnerabilidad permite a un atacante remoto comprometer el sistema objetivo. Existe debido a un error de uso de memoria luego de ser liberada, dentro del componente web apps de Google Chrome.

CVE-2021-4058: Esta vulnerabilidad permite a un atacante remoto comprometer el sistema objetivo. Existe debido a un error de límites de la memoria al procesar contenido HTML no confiable en ANGLE.

CVE-2021-4057: Esta vulnerabilidad permite a un atacante remoto comprometer el sistema objetivo. Existe debido a un error de uso de la memoria luego de ser liberada en el componente API en Google Chrome.

CVE-2021-4056: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. Existe debido a un error de confusión de tipo de archivo dentro del componente loader de Google Chrome.

CVE-2021-4055: Esta vulnerabilidad permite a un atacante remoto comprometer el sistema objetivo. Existe debido a un error de límites de la memoria al procesar contenido HTML no confiable en extensions.

CVE-2021-4054: Esta vulnerabilidad permite a un atacante remoto realizar un ataque de spoofing. La vulnerabilidad existe debido a una validación insuficiente al imput del usuario en autofill de Google Chrome.

CVE-2021-4053: Esta vulnerabilidad permite a un atacante remoto comprometer el sistema objetivo. Existe debido a un error de uso de la memoria luego de ser liberada en el componente UI en Google Chrome.

Productos afectados

Google Chrome, versiones 70.0.3538.67 a 96.0.4664.45.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

http://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4062
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4068
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4067
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4066
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4065
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4064
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4063
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4061
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4052
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4059
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4058
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4057
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4056
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4055
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4054
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4053

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.12.07 10:59:30 -03'00'