Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00617-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2022
Última revisión	12 de abril 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 del Gobierno de Chile, CSIRT de Gobierno, comparte nuevas vulnerabilidades comunicadas por Google para su navegador Chrome.

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

Vulnerabilidades

CVE-2022-1305
CVE-2022-1306
CVE-2022-1307
CVE-2022-1308
CVE-2022-1309
CVE-2022-1310
CVE-2022-1311
CVE-2022-1312
CVE-2022-1313
CVE-2022-1314

Impacto

Vulnerabilidades calificadas como de riesgo alto:

CVE-2022-1305 y CVE-2022-1312: Estas vulnerabilidades existen debido a un error de uso de memoria luego de ser liberada en el componente Storage en Google Chrome. Un atacante remoto puede crear una página web, engañar a su víctima para que haga clic, detonar el error y ejecutar código arbitrario en su sistema, comprometiéndolo.

CVE-2022-1308: Esta vulnerabilidad existe debido a un error de uso de memoria luego de ser liberada en el componente BFCache en Google Chrome. Un atacante remoto puede crear una página web,

engañar a su víctima para que haga clic, detonar el error y ejecutar código arbitrario en su sistema, comprometiéndolo.

CVE-2022-1309: Esta vulnerabilidad existe debido a un cumplimiento insuficiente de políticas en Developers Tools en Google Chrome. Permite a un atacante evadir las restricciones de seguridad implementadas. Un atacante puede engañar a la víctima para que visite un sitio especialmente diseñado, evadir las medidas de seguridad implementadas y comprometer el sistema afectado.

CVE-2022-1310: Esta vulnerabilidad existe debido a un error de uso de memoria luego de ser liberada en el componente Regular Expressions en Google Chrome. Un atacante remoto puede crear una página web, engañar a su víctima para que haga clic, detonar el error y ejecutar código arbitrario en su sistema, comprometiéndolo.

CVE-2022-1310: Esta vulnerabilidad existe debido a un error de uso de memoria luego de ser liberada en el componente Chrome Shell en Google Chrome. Un atacante remoto puede crear una página web, engañar a su víctima para que haga clic, detonar el error y ejecutar código arbitrario en su sistema, comprometiéndolo.

Productos afectados

Google Chrome: 70.0.3538.67 a 100.0.4896.75

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://chromereleases.googleblog.com/2022/04/stable-channel-update-for-desktop_11.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1306
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1307
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1308
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1309
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1310
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1311
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1312
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1313
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1314

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.04.12 17:09:47 -04'00'