Alerta de seguridad cibernética	9VSA21-00382-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de febrero de 2021
Última revisión	3 de febrero 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, CSIRT de Gobierno, comparte la información entregada por Google, sobre vulnerabilidades que afectan a Google Chrome.

Este informe incluye las medidas de mitigación, consistentes en instalar las actualizaciones de los productos afectados.

Vulnerabilidades

CVE-2021-21142
CVE-2021-21143
CVE-2021-21144
CVE-2021-21145
CVE-2021-21146
CVE-2021-21147

Impacto

CVE-2021-21142: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada en el componente Payments de Google Chrome. Un atacante remoto puede crear una página web, engañar a la víctima para que la visite, detonar un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-21143: Esta vulnerabilidad existe debido a un error de límites de memoria al procesar contenido HTML no confiable en Extensions. Un atacante remoto puede crear una página web, engañar a la víctima para que la visite, detonar un error de desbordamiento del buffer y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-21144: Esta vulnerabilidad existe debido a un error de límites de memoria al procesar contenido HTML no confiable en Tab Groups. Un atacante remoto puede crear una página web, engañar a la víctima para que la visite, detonar un error de desbordamiento del buffer y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-21145: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada en el componente Fonts de Google Chrome. Un atacante remoto puede crear una página web, engañar a la víctima para que la visite, detonar un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-21146: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada en el componente Navigation de Google Chrome. Un atacante remoto puede crear una página web, engañar a la víctima para que la visite, detonar un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-21147: Esta vulnerabilidad existe debido a una implementación incorrecta en Skia de Google Chrome. Un atacante remoto puede crear una página web, engañar a la víctima para que la visite, detonar un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

Productos afectados

Google Chrome, versiones de la 88.0.4324.0 a la 88.0.4324.145.

Mitigación

Instalar la actualización a la versión 88.0.4324.146 desde el sitio del proveedor.

Enlaces

https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21142

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21143

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21144

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21145

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21146

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21147

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.03 15:04:27 -03'00'