

Alerta de seguridad cibernética	9VSA21-00415-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2021
Última revisión	31 de marzo 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, comparte información sobre diez vulnerabilidades en Google Chrome.

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

Vulnerabilidades

CVE-2021-21194
CVE-2021-21195
CVE-2021-21196
CVE-2021-21197
CVE-2021-21198
CVE-2021-21199

También hay cuatro vulnerabilidades más que aún no cuentan con su propio CVE.

Impactos

Entre las vulnerabilidades sin CVE existen tres de riesgo alto, que permiten a un atacante remoto ejecutar código arbitrario en el sistema de la víctima, debido a un error al procesar contenido HTML, el que puede ser explotado por el atacante para detonar corrupción de memoria.

CVE-2021-21194 es considerada de alto riesgo, y permite a un atacante remoto comprometer los sistemas vulnerables debido a un error de memoria luego de ser liberada dentro del componente de captura de pantalla de Google Chrome.

CVE-2021-21195 es considerada de alto riesgo, y permite a un atacante remoto comprometer los sistemas vulnerables debido a un error de memoria luego de ser usada dentro del componente de V8 de Google Chrome.

CVE-2021-21196 es considerada de alto riesgo, y permite a un atacante remoto comprometer los sistemas vulnerables debido a un error de desbordamiento de buffer al procesar contenido HTML en TabStrip.

CVE-2021-21197 es considerada de alto riesgo, y permite a un atacante remoto comprometer los sistemas vulnerables debido a un error de límites de la memoria al procesar contenido HTML en TabStrip.

CVE-2021-21199 es considerada de alto riesgo, y permite a un atacante remoto comprometer los sistemas vulnerables debido a un error de memoria luego de ser liberada en Aura de Google Chrome.

Productos Afectados

Google Chrome, versiones de la 89.0.4389.0 a la 89.0.4386.113.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21194>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21195>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21196>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21197>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21198>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21199>