

Alerta de seguridad cibernética	9VSA21-00424-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2021
Última revisión	15 de abril 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 19 vulnerabilidades en la plataforma Google Chrome.

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

Vulnerabilidad

CVE-2021-21201	CVE-2021-21214	CVE-2021-21207
CVE-2021-21212	CVE-2021-21213	CVE-2021-21221
CVE-2021-21219	CVE-2021-21211	CVE-2021-21205
CVE-2021-21218	CVE-2021-21202	CVE-2021-21204
CVE-2021-21217	CVE-2021-21210	CVE-2021-21203
CVE-2021-21216	CVE-2021-21209	
CVE-2021-21215	CVE-2021-21208	

Impactos

Las vulnerabilidades consideradas como de riesgo alto son las siguientes:

CVE-2021-21201: Esta vulnerabilidad puede llevar a un atacante remoto a comprometer sistemas vulnerables. La vulnerabilidad tiene lugar debido a un error de uso de memoria luego de ser liberada dentro del componente de permisos en Google Chrome.

CVE-2021-21202: Esta vulnerabilidad puede llevar a un atacante remoto a comprometer sistemas vulnerables. La vulnerabilidad tiene lugar debido a un error de uso de memoria luego de ser liberada dentro del componente de extensiones en Google Chrome.

CVE-2021-21203, CVE-2021-21204: Estas vulnerabilidades puede llevar a un atacante remoto a comprometer sistemas vulnerables. La vulnerabilidad tiene lugar debido a un error de uso de memoria luego de ser liberada dentro del componente Blink en Google Chrome.

CVE-2021-21216 y CVE-2021-21215: Estas vulnerabilidades permiten a un atacante remoto ganar acceso a información sensible debido a una implementación incorrecta de Autofill en Google Chrome.

CVE-2021-21210: Esta vulnerabilidad permite a un atacante remoto ganar acceso a información sensible debido a una implementación incorrecta de Network en Google Chrome.

CVE-2021-21211: Esta vulnerabilidad permite a un atacante remoto ganar acceso a información sensible debido a una implementación incorrecta de Navigation en Google Chrome.

CVE-2021-21209: Esta vulnerabilidad permite a un atacante remoto ganar acceso a información sensible debido a una implementación incorrecta de storage en Google Chrome.

CVE-2021-21205: Esta vulnerabilidad permite a un atacante remoto evadir las restricciones de seguridad implementadas, debido a un cumplimiento insuficiente de las políticas en navegación en Google Chrome.

CVE-2021-21221: Esta vulnerabilidad permite a un atacante remoto ganar acceso a información sensible debido a una validación insuficiente de la información ingresada por el usuario en Mojo en Google Chrome.

Productos Afectados

Google Chrome, versiones 87.0.4280.66 a 89.0.4389.128

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21201>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21212>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21219>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21218>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21217>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21216>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21215>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21214>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21213>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21211>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21202>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21210>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21209>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21208>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21207>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21221>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21205>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21204>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21203>