

Alerta de seguridad cibernética	9VSA21-00354-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de enero de 2021
Última revisión	07 de enero 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 la información entregada por Google sobre 13 vulnerabilidades graves que afectan a su explorador web Google Chrome.

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

Vulnerabilidades

CVE-2021-21106
CVE-2021-21107
CVE-2021-21108
CVE-2021-21109
CVE-2021-21110
CVE-2021-21111
CVE-2021-21112
CVE-2021-21113
CVE-2020-16043
CVE-2021-21114
CVE-2020-15995
CVE-2021-21115
CVE-2021-21116

Impacto

CVE-2021-21106: Uso de memoria después de ser liberada en "Autocompletar".

Impacto: Alto

CVE-2021-21107: Uso de memoria después de ser liberada en "Drag and drop".

Impacto: Alto

CVE-2021-21108: Uso de memoria después de ser liberada en "media".

Impacto: Alto

CVE-2021-21109: Uso de memoria después de ser liberada en "pagos".

Impacto: Alto

CVE-2021-21110: Uso de memoria después de ser liberada en "Safe browsing".

Impacto: Alto

CVE-2021-21111: Insuficiente aplicación de las políticas en "WebUI".

Impacto: Alto

CVE-2021-21112: Uso de memoria después de ser liberada en "Blink".

Impacto: Alto

CVE-2021-21113: Desbordamiento del búfer en el heap en "Skia".

Impacto: Alto

CVE-2020-16043: Insuficiente validación de datos en "networking".

Impacto: Alto

CVE-2021-21114: Uso de memoria después de ser liberada en "audio".

Impacto: Alto

CVE-2020-15995: Escritura en memoria fuera de los límites en motor "V8".

Impacto: Alto

CVE-2021-21115: Uso de memoria después de ser liberada en "Safe browsing".

Impacto: Alto

CVE-2021-21116: Desbordamiento del búfer en el heap en "audio".

Impacto: Medio

Productos Afectados

Google Chrome versiones anteriores a la 87.0.4280.141 en Windows, Linux y Mac.

Mitigación

Las vulnerabilidades fueron mitigadas en la versión 87.0.4280.141 de Google Chrome para Windows, Linux y Mac.

Enlaces

<https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21106>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21107>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21108>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21109>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21110>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21111>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21112>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21113>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16043>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21114>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15995>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21115>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21116>