

Alerta de seguridad cibernética	9VSA20-00192-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de abril de 2020
Última revisión	29 de abril de 2020

## 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 afectada a actualizaciones.

## RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google referente a vulnerabilidades que afectan a Google Chrome. El presente informe incluye la respectiva medida de mitigación.

## VULNERABILIDADES

CVE-2020-6461  
CVE-2020-6462

## CVE-2020-6461

Debido a un error de uso de memoria luego de ser liberada en “almacenamiento”, un atacante remoto podría crear un sitio web especialmente diseñado, engañar a la víctima para que lo visite y así gatillar el error en memoria, comprometiendo completamente al sistema.

## CVE-2020-6462

Debido a un error de uso de memoria luego de ser liberada en “tareas programadas”, un atacante remoto podría crear un sitio web especialmente diseñado, engañar a la víctima para que lo visite y así gatillar el error en memoria, comprometiendo completamente al sistema.

### Productos Afectados

Google Chrome entre la versión 81.0.3988.0 hasta la 81.0.4044.128.

### Mitigación

Actualizar a la versión 81.0.4044.129 de Google Chrome.

### Enlaces

[https://chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop\\_27.html](https://chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop_27.html)

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6461>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6462>