

Alerta de seguridad cibernética	9VSA20-00250-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de junio de 2020
Última revisión	23 de junio 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 obtenida de Google referente a dos vulnerabilidades que afectan a su explorador web Google Chrome. El presente informe incluye la respectiva medida de mitigación.

## Vulnerabilidades

CVE-2020-6509

CWE-20

## Vulnerabilidades

CVE-2020-6509: Error de uso de memoria luego de ser liberada en las extensiones de Google Chrome permitiría a un atacante tomar control del sistema afectado.

Impacto: alto.

CWE-20: Debido a la insuficiente validación de datos ingresados por el usuario, un atacante podría realizar un ataque de ejecución de código remoto en el sistema afectado.

Impacto: alto.

### Productos Afectados

Google Chrome desde la versión 83.0.4103.0 hasta la 83.0.4103.115.

### Mitigación

Actualizar a la versión 83.0.4103.116 de Google Chrome.

### Enlaces

[https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop\\_22.html](https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop_22.html)

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6509>