

Alerta de seguridad informática	9VSA-00075-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2019
Última revisión	24 de octubre de 2019

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 en Google Chrome, junto a sus respectivas formas de mitigarlas.

Vulnerabilidades

CVE-2019-13699	CVE-2019-13709
CVE-2019-13700	CVE-2019-13710
CVE-2019-13701	CVE-2019-13711
CVE-2019-13702	CVE-2019-15903
CVE-2019-13703	CVE-2019-13713
CVE-2019-13704	CVE-2019-13714
CVE-2019-13705	CVE-2019-13715
CVE-2019-13706	CVE-2019-13716
CVE-2019-13707	CVE-2019-13718
CVE-2019-13708	

Impacto

- Uso de memoria luego de ser liberada en media
- Desbordamiento del buffer en Blink
- Falsificación de URL en navegación
- Escalación de privilegios en el instalador
- Suplantación de la barra de URL
- Bypass CSP
- Bypass en permiso de extensión
- Lectura fuera de límites en PDFium
- Exposición de información en almacenamiento de archivos
- Suplantación en la autenticación HTTP
- Bypass en la protección de descarga de archivos
- Exposición de información de contexto cruzado
- Desbordamiento de memoria en expat
- Exposición de información de origen cruzado
- Inyección CSS
- Suplantación de la barra de direcciones
- Error de estado en service worker
- Suplantación IDN

Productos Afectados

Todas las versiones anteriores a Google Chrome 78.0.3904.70.

Mitigación

Actualizar a la versión 78.0.3904.70.

Enlace

- https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_22.html
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13699>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13700>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13701>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13702>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13703>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13704>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13705>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13706>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13707>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13708>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13709>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13710>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13711>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13713>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13714>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13715>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13716>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-13718>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-15903>