Alerta de seguridad cibernética	9VSA20-00303-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de octubre de 2020
Última revisión	15 de octubre 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 afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de Google respecto a múltiples vulnerabilidades que afectan a su explorador web Google Chrome. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-15960
CVE-2020-15961
CVE-2020-15962
CVE-2020-15963
CVE-2020-15964
CVE-2020-15965
CVE-2020-15966
CVE-2020-6573
CVE-2020-6574
CVE-2020-6575
CVE-2020-6576

Impactos

CVE-2020-15960: Lectura fuera de los límites de la memoria en Almacenamiento.
Impacto: Alto
CVE-2020-15961: Insuficiente aplicación de políticas en Extensiones.
Impacto: Alto
CVE-2020-15962: Insuficiente aplicación de políticas en “Serial”.
Impacto: Alto
CVE-2020-15963: Insuficiente aplicación de políticas en Extensiones.
Impacto: Alto
CVE-2020-15964: Insuficiente validación de datos en Media.
Impacto: Bajo
CVE-2020-15965: Escritura fuera de los límites de la memoria en motor V8.
Impacto: Alto
CVE-2020-15966: Insuficiente aplicación de políticas en Extensiones.
Impacto: Medio

Productos Afectados

Google Chrome versiones anteriores a la 85.0.4183.121.

Mitigación

Las vulnerabilidades fueron mitigadas en la versión 85.0.4183.121 de Google Chrome para Windows, Linux y Mac.

Enlaces

https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop_21.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15966

Impactos

CVE-2020-6573: Uso de memoria después de ser liberada en video.
Impacto: Alto
CVE-2020-6574: Insuficiente aplicación de políticas en instalador.
Impacto: Alto
CVE-2020-6575: Condición de carrera en “Mojo”.
Impacto: Alto
CVE-2020-6576: Uso de memoria después de ser liberada en “Offscreen canvas”.

Impacto: Alto
CVE-2020-15959: Insuficiente aplicación de políticas en Networking.
Impacto: Alto

Productos Afectados

Google Chrome versiones anteriores a la 85.0.4183.102.

Mitigación

Las vulnerabilidades fueron mitigadas en la 85.0.4183.102 de Google Chrome para Windows, Linux y Mac.

Enlaces

https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6573
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6574
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6575
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6576
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15959

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.10.15 12:28:16 -03'00'