Alerta de seguridad cibernética	9VSA20-00296-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de septiembre de 2020
Última revisión	07 de septiembre 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 al explorador web Google Chrome. El presente informe incluye medidas de mitigación.

Vulnerabilidades

CVE-2020-6563
CVE-2020-6571
CVE-2020-6570
CVE-2020-6569
CVE-2020-6568
CVE-2020-6567
CVE-2020-6566
CVE-2020-6565
CVE-2020-6564
CVE-2020-6562
CVE-2020-6561
CVE-2020-6560
CVE-2020-6559
CVE-2020-6558

Impactos

CVE-2020-6563: Insuficiente aplicación de políticas en gestor de “intents”.
Impacto: Medio
CVE-2020-6571: Seguridad en interfaz de usuario incorrecta en “Omnibox”.
Impacto: Bajo
CVE-2020-6570: Filtración de información en canal lateral en “WebRTC”.
Impacto: Bajo.
CVE-2020-6569: Desbordamiento de un entero en memoria en “WebUSB”.
Impacto: Bajo.
CVE-2020-6568: Insuficiente aplicación de políticas en gestor de “intents”.
Impacto: Bajo.
CVE-2020-6567: Insuficiente validación de datos no confiables ingresados por un usuario en el gestor de la línea de comandos.
Impacto: Bajo.
CVE-2020-6566: Insuficiente aplicación de políticas en “media”.
Impacto: Medio.
CVE-2020-6565: Seguridad en interfaz de usuario incorrecta en “Omnibox”.
Impacto: Medio.
CVE-2020-6564: Seguridad en interfaz de usuario incorrecta en “Permisos”.
Impacto: Medio.
CVE-2020-6562: Insuficiente aplicación de políticas en “Blink”.
Impacto: Medio.
CVE-2020-6561: Inapropiada implementación en CSP (Content Security Policy).
Impacto: Medio.
CVE-2020-6560: Insuficiente aplicación de políticas en “autofill”.
Impacto: Medio.
CVE-2020-6559: Uso de memoria después de ser liberada en “Presentation API”.
Impacto: Alto.
CVE-2020-6558: Insuficiente aplicación de políticas en “iOS”.
Impacto: Alto.

Productos Afectados

Google Chrome versiones anteriores a la 85.0.4183.83.

Mitigaciones

Actualizar Google Chrome a la versión 85.0.4183.83.

Enlaces

https://chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop_25.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6563
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6571
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6570
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6569
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6568
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6567
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6566
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6565
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6564
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6562
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6561
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6560
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6559
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6558