Alerta de seguridad cibernética	9VSA20-00325-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2020
Última revisión	23 de noviembre 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 para Escritorio. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-16018
CVE-2020-16019
CVE-2020-16020
CVE-2020-16021
CVE-2020-16022
CVE-2020-16015
CVE-2020-16014
CVE-2020-16023
CVE-2020-16024
CVE-2020-16025
CVE-2020-16026
CVE-2020-16027
CVE-2020-16028
CVE-2020-16029
CVE-2020-16030
CVE-2019-8075
CVE-2020-16031
CVE-2020-16032
CVE-2020-16033
CVE-2020-16034
CVE-2020-16035
CVE-2020-16012
CVE-2020-16036

Impactos

CVE-2020-16018: Uso de memoria después de ser liberada en Payments.
Impacto: Alto

CVE-2020-16019: Implementación inapropiada en Filesystem.
Impacto: Alto

CVE-2020-16020: Implementación inapropiada en Cryptohome.
Impacto: Alto

CVE-2020-16021: Condición de carrera en ImageBurner.
Impacto: Alto

CVE-2020-16022: Insuficiente aplicación de políticas en Networking.
Impacto: Alto

CVE-2020-16015: Insuficiente validación de datos ingresados por un usuario en WASM.
Impacto: Alto

CVE-2020-16014: Uso de memoria después de ser liberada en PPAPI.
Impacto: Alto

CVE-2020-16023: Uso de memoria después de ser liberada en WebCodecs.
Impacto: Alto

CVE-2020-16024: Desbordamiento del búfer en el montículo en UI.
Impacto: Alto

CVE-2020-16025: Desbordamiento del búfer en el montículo en Uclipboard.
Impacto: Alto

CVE-2020-16026: Uso de memoria después de ser liberada en WebRTC.
Impacto: Medio

CVE-2020-16027: Insuficiente aplicación de políticas en Developer tools.
Impacto: Medio

CVE-2020-16028: Desbordamiento del búfer en el montículo en UWebRTC.
Impacto: Medio

CVE-2020-16029: Implementación inapropiada en PDFium.
Impacto: Medio

CVE-2020-16030: Insuficiente validación de datos ingresados por un usuario en Blink.
Impacto: Medio

CVE-2019-8075: Insuficiente validación de datos ingresados por un usuario en Flash.
Impacto: Medio

CVE-2020-16031: Incorrecta seguridad de interfaz de usuario en Tab preview.
Impacto: Medio

CVE-2020-16032: Incorrecta seguridad de interfaz de usuario en Sharing.
Impacto: Medio

CVE-2020-16033: Incorrecta seguridad de interfaz de usuario en WebUSB.
Impacto: Medio

CVE-2020-16034: Implementación inapropiada en WebRTC.
Impacto: Medio

CVE-2020-16035: Insuficiente validación de datos ingresados por un usuario en Cros-disks.
Impacto: Medio

CVE-2020-16012: Filtración de información de canal lateral en Graphics.
Impacto: Bajo

CVE-2020-16036: Implementación inapropiada en Cookies.
Impacto: Bajo

Productos Afectados

Google Chrome versiones anteriores a la 87.0.4280.66 en Windows y Linux, y 87.0.4280.67 en Mac.

Mitigación

Las vulnerabilidades fueron mitigadas en la versión 87.0.4280.66 de Google Chrome para Windows y Linux, y en la versión 87.0.4280.67 para Mac.

Enlaces

https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_17.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16024

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16025
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16026
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16029
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16030
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8075
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16031
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16034
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16035
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16036