Alerta de seguridad cibernética	9VSA20-00273-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de julio de 2020
Última revisión	17 de julio 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 las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2020-6510
CVE-2020-6511
CVE-2020-6512
CVE-2020-6513
CVE-2020-6514
CVE-2020-6515
CVE-2020-6516
CVE-2020-6517
CVE-2020-6518
CVE-2020-6519
CVE-2020-6520
CVE-2020-6521
CVE-2020-6522
CVE-2020-6523
CVE-2020-6524
CVE-2020-6525
CVE-2020-6526
CVE-2020-6527
CVE-2020-6528
CVE-2020-6529
CVE-2020-6530
CVE-2020-6531
CVE-2020-6533
CVE-2020-6534
CVE-2020-6535
CVE-2020-6536

Vulnerabilidades

CVE-2020-6510: Desbordamiento del buffer del montículo en búsquedas de fondo. Impacto: Crítico.
CVE-2020-6511: Filtración de información de canal lateral en políticas de seguridad de contenido (Content Security Policy). Impacto: Alto.
CVE-2020-6512: Confusión de tipo en motor V8. Impacto: Alto.
CVE-2020-6513: Desbordamiento del buffer del montículo en PDFium. Impacto: Alto.
CVE-2020-6514: Inapropiada implementación en WebRTC. Impacto: Alto.
CVE-2020-6515: Uso de memoria luego de ser liberada en la tira de pestañas del navegador. Impacto: Alto.
CVE-2020-6516: Evasión de políticas en CORS. Impacto: Alto.
CVE-2020-6517: Desbordamiento del buffer del montículo en historial. Impacto: Alto.
CVE-2020-6518: Uso de memoria después de ser liberada en herramientas de desarrollador. Impacto: Medio.
CVE-2020-6519: Evasión de políticas en políticas de seguridad de contenido (Content Security Policy). Impacto: Medio.
CVE-2020-6520: Desbordamiento del buffer del montículo en Skia. Impacto: Medio.
CVE-2020-6521: Filtración de información de canal lateral en auto rellenar. Impacto: Medio.
CVE-2020-6522: Inapropiada implementación en manejadores de protocolos externos. Impacto: Medio.
CVE-2020-6523: Escritura en memoria fuera de los límites en Skia. Impacto: Medio.
CVE-2020-6524: Desbordamiento del buffer del montículo en WebAudio. Impacto: Bajo.
CVE-2020-6525: Desbordamiento del buffer del montículo en Skia. Impacto: Bajo.
CVE-2020-6526: Inapropiada implementación en iframe sandbox. Impacto: Bajo.
CVE-2020-6527: Insuficiente aplicación de políticas en políticas de seguridad de contenido (Content Security Policy). Impacto: Bajo.
CVE-2020-6528: Incorrecta interfaz de seguridad de usuario en autenticación básica. Impacto: Bajo.
CVE-2020-6529: Inapropiada implementación en WebRTC. Impacto: Bajo.
CVE-2020-6530: Acceso a locaciones de memoria fuera de los límites en herramientas de desarrollador. Impacto: Bajo.
CVE-2020-6531: Filtración de información de canal lateral en desplazar texto. Impacto: Bajo.
CVE-2020-6533: Confusión de tipo en motor V8. Impacto: Bajo.
CVE-2020-6534: Desbordamiento del buffer del montículo en WebRTC. Impacto: Bajo.
CVE-2020-6535 Insuficiente validación de datos en WebUI. Impacto: Bajo.
CVE-2020-6536: Incorrecta interfaz de seguridad de usuario en PWAs. Impacto: Bajo.

Productos Afectados

Actualizar a la versión 84.0.4147.89 de Google Chrome.

Mitigaciones

Google Chrome versiones anteriores a la 84.0.4147.89.

Enlaces

https://chromereleases.googleblog.com/2020/07/stable-channel-update-for-desktop.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6510

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6511
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6512
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6513
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6515
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6516
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6517
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6518
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6519
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6520
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6521
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6522
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6523
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6524
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6525
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6526
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6527
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6528
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6529
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6530
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6531
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6533
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6534
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6535
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6536