Alerta de seguridad informática	9VSA20-00218-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2020
Última revisión	20 de mayo 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 referente a múltiples vulnerabilidades que afectan a su explorador web. El presente informe incluye la respectiva medida de mitigación.

Lista de CVEs

CVE-2020-6465
CVE-2020-6466
CVE-2020-6467
CVE-2020-6468
CVE-2020-6469
CVE-2020-6470
CVE-2020-6471
CVE-2020-6472
CVE-2020-6473
CVE-2020-6474
CVE-2020-6475
CVE-2020-6476
CVE-2020-6477
CVE-2020-6478
CVE-2020-6479
CVE-2020-6480
CVE-2020-6481
CVE-2020-6482
CVE-2020-6483
CVE-2020-6484
CVE-2020-6485
CVE-2020-6486
CVE-2020-6487
CVE-2020-6488
CVE-2020-6489
CVE-2020-6490
CVE-2020-6491

Vulnerabilidades

CVE-2020-6465: Error de uso de memoria luego de ser liberada en el modo lectura.
Permitiría a un atacante la ejecución de código remoto a través de un sitio web especialmente diseñado, comprometiendo completamente al sistema afectado.

CVE-2020-6466: Error de uso de memoria luego de ser liberada en el "media".
Permitiría a un atacante la ejecución de código remoto a través de un sitio web especialmente diseñado, comprometiendo completamente al sistema afectado.

CVE-2020-6467: Error de uso de memoria luego de ser liberada en el "WebRTC".
Permitiría a un atacante la ejecución de código remoto a través de un sitio web especialmente diseñado, comprometiendo completamente al sistema afectado.

CVE-2020-6468: Error de confusión de tipo en componente V8.
Permitiría a un atacante la ejecución de código remoto a través de un sitio web especialmente diseñado, comprometiendo completamente al sistema afectado.

CVE-2020-6469: Insuficiente aplicación de las políticas en las herramientas de desarrollador.
Permitiría a un atacante comprometer al sistema afectado a través de un sitio web especialmente diseñado.

CVE-2020-6470: Insuficiente validación de datos no confiables en el portapapeles.
Permitiría a un atacante obtener información sensible a través de un sitio web especialmente diseñado.

CVE-2020-6471: Insuficiente aplicación de las políticas en las herramientas de desarrollador.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6472: Insuficiente aplicación de las políticas en las herramientas de desarrollador.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6473: Insuficiente aplicación de las políticas en "Blink".
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6474: Error de uso de memoria luego de ser liberada en "Blink".
Permitiría a un atacante obtener información sensible a través de un sitio web especialmente diseñado.

CVE-2020-6475: Interfaz de usuario insegura en modo pantalla completa.
Permitiría a un atacante suplantar el contenido del sitio en modo pantalla completa a través de un sitio web especialmente diseñado.

CVE-2020-6476: Insuficiente aplicación de las políticas en las pestañas del explorador.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6477: Implementación inadecuada en el instalador.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6478: Implementación inadecuada en el modo pantalla completa.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6479: Implementación inadecuada en la funcionalidad compartir.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6480: Insuficiente aplicación de las políticas en “Enterprise”.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6481: Insuficiente aplicación de las políticas en el formateo de URLs.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6482: Insuficiente aplicación de las políticas en las herramientas de desarrollador.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6483: Insuficiente aplicación de las políticas en la funcionalidad pagos.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6484: Insuficiente validación de datos en el componente “ChromeDriver”.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6485: Insuficiente validación de datos en el componente “media router”.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6486: Insuficiente aplicación de las políticas en “navigations”.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información sensible.

CVE-2020-6487: Insuficiente aplicación de las políticas en descargas.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información potencialmente sensible.

CVE-2020-6488: Insuficiente aplicación de las políticas en descargas.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información potencialmente sensible.

CVE-2020-6489: Implementación inadecuada en las herramientas de desarrollador.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información potencialmente sensible.

CVE-2020-6490: Insuficiente validación de datos en “loader”.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información potencialmente sensible.

CVE-2020-6491: Seguridad de interfaz de usuario incorrecta en información de sitio.
Permitiría a un atacante evadir medidas de seguridad a través de un sitio web especialmente diseñado, para obtener información potencialmente sensible.

Productos Afectados
Google Chrome desde la versión 83.0.4103.0 hasta la 83.0.4103.60.

Mitigación
Actualizar a la versión 83.0.4103.61 de Google Chrome.

Enlaces
https://chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop_19.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6465
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6466
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6467
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6468
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6469
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6470
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6471
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6472
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6473
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6474
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6475
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6477
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6478
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6479
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6480

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6481
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6482
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6483
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6484
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6485
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6486
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6487
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6488
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6489
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6490
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6491