| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00524-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 25 de noviembre de 2021 |
| Última revisión | 25 de noviembre de 2021 |

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 del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades conocidas en Microsoft Edge.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

## Vulnerabilidades

CVE-2021-38012
CVE-2021-43221
CVE-2021-38005
CVE-2021-38006
CVE-2021-38007
CVE-2021-38008
CVE-2021-38009
CVE-2021-38010
CVE-2021-42308
CVE-2021-38013
CVE-2021-38011
CVE-2021-38014
CVE-2021-38015
CVE-2021-38016
CVE-2021-38017
CVE-2021-38018
CVE-2021-38019
CVE-2021-38020
CVE-2021-38021
CVE-2021-38022

## Impactos

Vulnerabilidades de riesgo alto:

CVE-2021-38005: Permite que un atacante remoto ponga en peligro a un sistema vulnerable, debido a un error de uso de memoria después de ser liberada, dentro del componente loader en Microsoft Edge.

CVE-2021-38006: Permite que un atacante remoto ponga en peligro a un sistema vulnerable, debido a un error de uso de memoria después de ser liberada, dentro del componente storage foundation en Microsoft Edge.

CVE-2021-38007: Permite que un atacante remoto haga ejecución arbitraria de código en el sistema de destino, debido a un error de confusión de tipos de memoria dentro del componente V8 en Microsoft Edge.

CVE-2021-38008: Permite que un atacante remoto ponga en peligro a un sistema vulnerable, debido a un error de uso de memoria después de ser liberada, dentro del componente multimedia en Microsoft Edge.

CVE-2021-38011: Permite que un atacante remoto ponga en peligro a un sistema vulnerable, debido a un error de uso de memoria después de ser liberada, dentro del componente storage foundation en Microsoft Edge.

CVE-2021-38015: Permite que un atacante remoto obtenga acceso a información confidencial, debido a una implementación incorrecta en los inputs 28en Microsoft Edge.

CVE-2021-38018: La vulnerabilidad permite que un atacante remoto obtenga acceso a información confidencial, debido a una implementación incorrecta en Navegación en Microsoft Edge.

CVE-2021-38021: La vulnerabilidad permite que un atacante remoto obtenga acceso a información confidencial, debido a una implementación incorrecta en Referrer en Microsoft Edge.

Vulnerabilidades de riesgo medio:

CVE-2021-38012: La vulnerabilidad permite que un atacante remoto obtenga acceso a información potencialmente sensible, debido a un error de confusión de tipos de memoria dentro del componente V8 en Microsoft Edge.

CVE-2021-38009: La vulnerabilidad permite que un atacante remoto ponga en peligro un sistema afectado, debido a una implementación incorrecta en la caché en Microsoft Edge.

CVE-2021-38010: La vulnerabilidad permite que un atacante remoto ponga en peligro un sistema afectado, debido a una implementación incorrecta en Service Workers en Microsoft Edge.

CVE-2021-38013: Permite que un atacante remoto ponga en peligro un sistema vulnerable, debido a un error de límites de memoria al procesar contenido HTML que no es de confianza en el reconocimiento de huellas dactilares.

CVE-2021-38014: Permite que un atacante remoto ponga en peligro un sistema vulnerable, debido a un error de límite al procesar contenido HTML que no es de confianza en Swiftshader.

CVE-2021-38016: La vulnerabilidad permite que un atacante remoto eluda las restricciones de seguridad implementadas, debido a la aplicación insuficiente de políticas en la búsqueda en segundo plano en Microsoft Edge.

CVE-2021-38017: La vulnerabilidad permite que un atacante remoto eluda las restricciones de seguridad implementadas, debido a la aplicación insuficiente de políticas en la zona de pruebas de iframe en Microsoft Edge.

CVE-2021-38019: La vulnerabilidad permite que un atacante remoto eluda las restricciones de seguridad implementadas, debido a una aplicación insuficiente de políticas en CORS en Microsoft Edge.

CVE-2021-38020: La vulnerabilidad permite que un atacante remoto eluda las restricciones de seguridad implementadas, debido a la aplicación insuficiente de políticas en el selector de contactos en Microsoft Edge.

### Vulnerabilidades de riesgo bajo:

CVE-2021-43221: La vulnerabilidad permite que un atacante remoto ejecute código arbitrario en el sistema de destino, debido a una validación incorrecta de entradas.

CVE-2021-42308: La vulnerabilidad permite que un atacante remoto realice un ataque de suplantación de identidad, debido al procesamiento incorrecto de los datos proporcionados por el usuario.

CVE-2021-38022: La vulnerabilidad permite que un atacante remoto obtenga acceso a información confidencial, debido a una implementación incorrecta en WebAuthentication en Microsoft Edge.

### Productos Afectados
Microsoft Edge: 79.0.309.71 a 95.0.1020.53

### Mitigación
Instalar las respectivas actualizaciones entregadas por el proveedor.

### Enlaces
https://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43221
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42308
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38015

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38022

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.11.25 21:44:47 -03'00'