

|              |   |  |   |
|--------------|---|--|---|
| Nro. Alerta: | EC-2022-25  | CENTRO DE RESPUESTA A INCIDENTES<br>INFORMÁTICOS<br><b>ALERTA DE SEGURIDAD</b> |  |
| TLP:         |  |  |   |
| Fecha:       | 08-febrero-2022   | <b>Múltiples vulnerabilidades en Microsoft Edge</b>                            | Versión 1.0   |

## I. DATOS GENERALES:

|                           |                              |
|---------------------------|------------------------------|
| <b>Clase de alerta:</b>   | Vulnerabilidad               |
| <b>Tipo de incidente:</b> | Sistema y/o Software Abierto |
| <b>Nivel de riesgo:</b>   | Alto                         |

## II. ALERTA

Se han descubierto múltiples vulnerabilidades en el navegador Microsoft Edge que permitirían a un atacante remoto provocar una condición de denegación de servicio, elevación de privilegios, ejecución remota de código, divulgación de información confidencial, manipulación de datos y omisión de restricciones de seguridad en el sistema objetivo.



**Figura 1.** Ilustración representativa de Microsoft Edge  
*Fuente: Microsoft*

## III. INTRODUCCIÓN

Chromium es un proyecto de navegador de código abierto que tiene como objetivo crear una forma más segura, rápida y estable para que todos los usuarios experimenten la web; aprovechando estas características, diferentes navegadores Web son basados en Chromium, entre los que se menciona:

- Chrome.
- Edge.
- Brave.
- Opera.
- SRWare Iron.
- Torch.
- Vivaldi.



|              |   |  |   |
|--------------|---|--|---|
| Nro. Alerta: | EC-2022-25  | CENTRO DE RESPUESTA A INCIDENTES<br>INFORMÁTICOS<br><b>ALERTA DE SEGURIDAD</b> |  |
| TLP:         |  |  |   |
| Fecha:       | 08-febrero-2022   | <b>Múltiples vulnerabilidades en Microsoft Edge</b>                            | Versión 1.0   |

- Yandex Browser.

Considerando lo manifestado anteriormente, Microsoft Edge es un navegador Web desarrollado por Microsoft, basado en Chromium, la fecha de lanzamiento para Windows 10 fue en 2015, mientras que para IOS y Android fue en el 2017.

En este sentido, el Centro de respuestas de seguridad de Microsoft; cuyo objetivo es investigar los diferentes informes de vulnerabilidades de seguridad que afectan a los productos y servicios de Microsoft, ha dado a conocer vulnerabilidades asociadas al navegador Microsoft Edge en versiones anteriores a 98.0.1108.43.

#### IV. VECTOR DE ATAQUE:

Los componentes vulnerables están vinculados a la red o son explotables de forma remota, estas vulnerabilidades presentan las siguientes características:

- La explotación no necesita ninguna autenticación específica.
- La explotación exitosa requiere la interacción del usuario por parte de la víctima

En la siguiente tabla se mencionan las diferentes vulnerabilidades y sus características técnicas:

| CVE            | DESCRIPCIÓN   |
|----------------|---|
| CVE-2022-23261 | La vulnerabilidad permite que un atacante remoto realice un ataque de suplantación de identidad.  |
| CVE-2022-23262 | La vulnerabilidad permite que un atacante remoto ejecute código arbitrario en el sistema de destino.  |
| CVE-2022-23263 | Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, desencadenar un error de uso después de liberar y obtener acceso a información confidencial. |

**Tabla 1.** Características Técnicas Vulnerabilidades Navegador Microsoft Edge.

Considerando que Microsoft Edge es basado en Chromium; es importante mencionar que existen CVE asignadas por Chrome; las mismas que se mencionan a continuación.

| CVE           | DESCRIPCIÓN   |
|---------------|---|
| CVE-2022-0452 | La vulnerabilidad permite que un atacante remoto comprometa un sistema vulnerable.  |
| CVE-2022-0453 | Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, desencadenar un error de uso después de libre y ejecutar código arbitrario en el sistema de destino. |



|              |   |  |   |
|--------------|---|--|---|
| Nro. Alerta: | EC-2022-25  | CENTRO DE RESPUESTA A INCIDENTES<br>INFORMÁTICOS<br><b>ALERTA DE SEGURIDAD</b> |  |
| TLP:         |  |  |   |
| Fecha:       | 08-febrero-2022   | <b>Múltiples vulnerabilidades en Microsoft Edge</b>                            | Versión 1.0   |

| CVE           | DESCRIPCIÓN   |
|---------------|---|
|               | La explotación exitosa de la vulnerabilidad puede permitir que un atacante comprometa un sistema vulnerable.  |
| CVE-2022-0454 | La vulnerabilidad permite que un atacante remoto comprometa un sistema vulnerable.  |
| CVE-2022-0455 | La vulnerabilidad permite que un atacante remoto comprometa el sistema afectado.  |
| CVE-2022-0456 | La vulnerabilidad permite que un atacante remoto comprometa un sistema vulnerable.  |
| CVE-2022-0457 | La vulnerabilidad permite que un atacante remoto ejecute código arbitrario en el sistema de destino.  |
| CVE-2022-0458 | Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, desencadenar un error de uso después de libre y ejecutar código arbitrario en el sistema de destino. |
| CVE-2022-0459 | Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, desencadenar un error de uso después de libre y ejecutar código arbitrario en el sistema de destino  |
| CVE-2022-0460 | Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, desencadenar un error de uso después de liberar y obtener acceso a información confidencial.                   |
| CVE-2022-0461 | La vulnerabilidad permite a un atacante remoto eludir las restricciones de seguridad implementadas  |
| CVE-2022-0462 | Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y obtener acceso a información confidencial.  |
| CVE-2022-0464 | La vulnerabilidad permite que un atacante remoto comprometa un sistema vulnerable   |
| CVE-2022-0465 | Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, desencadenar un error de uso después de liberar y obtener acceso a información confidencial.                   |
| CVE-2022-0466 | Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y obtener acceso a información confidencial.  |
| CVE-2022-0467 | La vulnerabilidad permite que un atacante remoto obtenga acceso a información confidencial.   |
| CVE-2022-0468 | La vulnerabilidad permite que un atacante remoto comprometa un sistema vulnerable.  |



|              |  |  |   |
|--------------|--|--|---|
| Nro. Alerta: | EC-2022-25   | CENTRO DE RESPUESTA A INCIDENTES<br>INFORMÁTICOS<br><b>ALERTA DE SEGURIDAD</b> |  |
| TLP:         | <br><b>TLP:BLANCO</b> |  |   |
| Fecha:       | 08-febrero-2022  | <b>Múltiples vulnerabilidades en Microsoft Edge</b>                            | Versión 1.0   |

| CVE           | DESCRIPCIÓN   |
|---------------|---|
| CVE-2022-0469 | Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, desencadenar un error de uso después de liberar y obtener acceso a información confidencial. |
| CVE-2022-0470 | La vulnerabilidad permite que un atacante remoto obtenga acceso para bloquear el navegador.   |

**Tabla 2.** Características Técnicas Vulnerabilidades asignadas por Chrome.  
**Fuente:** Alerta EcuCERT EC-2022-22\_GOOGLE\_CHROME\_V1

## V. IMPACTO:

A continuación, se menciona el impacto de las diferentes vulnerabilidades:

| CVE            | IMPACTO  | RIESGO |
|----------------|--|--------|
| CVE-2022-23261 | <b>Confidencialidad:</b> Ninguno<br><b>Integridad:</b> Bajo<br><b>Disponibilidad:</b> Ninguno                      | BAJO   |
| CVE-2022-23262 | <b>Confidencialidad:</b> Bajo<br><b>Integridad:</b> Bajo<br><b>Disponibilidad:</b> Bajo<br>Elevación de privilegio | MEDIO  |
| CVE-2022-23263 | <b>Confidencialidad:</b> Alto<br><b>Integridad:</b> Alto<br><b>Disponibilidad:</b> Alto<br>Elevación de privilegio | MEDIO  |

**Tabla 3.** Impacto Vulnerabilidades Navegador Microsoft Edge.

## VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Descargar programas y archivos de fuentes oficiales.
- Actualizar el Navegador Microsoft Edge a la versión 98.0.1108.43 o posterior.

## VII. REFERENCIAS:



<https://www.ecucert.gob.ec>



@EcuCERT\_EC

Pág.: 4 of 5

|              |  |  |   |
|--------------|--|--|---|
| Nro. Alerta: | EC-2022-25   | CENTRO DE RESPUESTA A INCIDENTES<br>INFORMÁTICOS<br><b>ALERTA DE SEGURIDAD</b> |  |
| TLP:         | <br><b>TLP:BLANCO</b> |  |   |
| Fecha:       | 08-febrero-2022  | <b>Múltiples vulnerabilidades en Microsoft Edge</b>                            | Versión 1.0   |

Chromium. (s.f.). *Chromium*. Obtenido de Chromium: <https://www.chromium.org/chromium-projects/>

EcuCERT. (04 de 02 de 2022). EcuCERT. Obtenido de EcuCERT: [https://www.ecucert.gob.ec/wp-content/uploads/2022/02/EC-2022-22\\_GOOGLE\\_CHROME\\_V1.pdf](https://www.ecucert.gob.ec/wp-content/uploads/2022/02/EC-2022-22_GOOGLE_CHROME_V1.pdf)

Hkcert. (04 de 02 de 2022). *Hkcert*. Obtenido de Hkcert: [https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities\\_20220204](https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20220204)

Microsoft. (s.f.). *Microsoft*. Obtenido de Microsoft: <https://www.microsoft.com/es-es/edge>

Microsoft, M. (03 de 02 de 2022). *Msrc Microsoft*. Obtenido de Msrc Microsoft: <https://msrc.microsoft.com/update-guide/vulnerability>

Msrc.microsoft. (02 de 02 de 2022). *Msrc.microsoft*. Obtenido de Msrc.microsoft: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23261>

Msrc.microsoft. (03 de 02 de 2022). *Msrc.microsoft*. Obtenido de Msrc.microsoft: <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-23262>

Msrc.microsoft. (03 de 02 de 2022). *Msrc.microsoft*. Obtenido de Msrc.microsoft: <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-23263>

Serrano, I. (19 de 07 de 2021). *Adslzone*. Obtenido de Adslzone: <https://www.adslzone.net/reportajes/software/navegadores-chromium/>

Vuldb. (07 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: <https://vuldb.com/?id.192445>

Vuldb. (07 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: <https://vuldb.com/?id.192446>

Vuldb. (07 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: <https://vuldb.com/?id.192447>

