

Alerta de seguridad cibernética	9VSA21-00428-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	23 de abril de 2021
Última revisión	23 de abril 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, CSIRT de Gobierno, comparte información sobre varias vulnerabilidades críticas en Microsoft Edge.

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

Vulnerabilidades

CVE-2021-21222
CVE-2021-21223
CVE-2021-21224
CVE-2021-21225
CVE-2021-21226

Impactos

CVE-2021-21224: La vulnerabilidad es del tipo error por confusión de tipo de archivo, y tiene lugar en el motor de búsqueda V8 JavaScript de código abierto. Esta vulnerabilidad permite a un atacante remoto comprometer un sistema vulnerable.

Esta vulnerabilidad está siendo activamente explotada

CVE-2021-21223: Esta vulnerabilidad ocurre por un error de desbordamiento de enteros en el motor de búsqueda V8. Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario.

CVE-2021-21225: Esta vulnerabilidad existe debido a un error de límites de la memoria al procesar datos ingresados no confiables dentro del motor de búsqueda V8. Esta vulnerabilidad permite a un atacante remoto comprometer un sistema desprotegido.

CVE-2021-21222: Esta vulnerabilidad existe debido a un error de límites de la memoria al procesar contenido HTML no confiable dentro del motor de búsqueda V8. Esta vulnerabilidad permite a un atacante remoto comprometer un sistema desprotegido.

CVE-2021-21226: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada dentro del componente de navegación de Google Chrome. Esta vulnerabilidad permite a un atacante remoto comprometer un sistema desprotegido.

Productos Afectados

Microsoft Edge, versiones de la 79.0.309.71 a la 90.0.818.39.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor cuando estén disponibles.

Enlaces

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-21224>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-21222>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-21223>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-21225>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-21226>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21224>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21222>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21223>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21225>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21226>