

Alerta de seguridad cibernética	9VSA21-00425-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de abril de 2021
Última revisión	20 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 vulnerabilidades en Mozilla Thunderbird, Firefox y Firefox ESR.

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

Vulnerabilidad

CVE-2021-23994	CVE-2021-24002	CVE-2021-23997
CVE-2021-23995	CVE-2021-29945	CVE-2021-24000
CVE-2021-23998	CVE-2021-29946	CVE-2021-24001
CVE-2021-23961	CVE-2021-29948	CVE-2021-29947
CVE-2021-23999	CVE-2021-23996	

Impactos

Las vulnerabilidades consideradas como de riesgo alto son las siguientes:

CVE-2021-23994: Esta vulnerabilidad existe debido a un error de límites de la memoria al procesar información no confiable ingresada dentro del framebuffer de WebGL. Un atacante remoto puede crear una página web y engañar a la víctima para que la abra usando el software afectado, detonando escritura fuera de límites y ejecutando código arbitrario en el sistema objetivo.

CVE-2021-23995: Esta vulnerabilidad existe debido a un error de límites de la memoria al procesar información no confiable ingresada, cuando el Responsive Design Mode está activado. Un atacante

remoto puede crear una página web y engañar a la víctima para que la abra usando el software afectado, detonando escritura fuera de límites y ejecutando código arbitrario en el sistema objetivo.

Productos Afectados

Mozilla Thunderbird: versiones de la 60.0 a la 78.9.1.

Mozilla Firefox: versiones de la 8.0.1 a la 87.0.

Mozilla Firefox ESR: versiones de la 60.0 a la 78.9.1.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

<https://www.mozilla.org/en-US/security/advisories/mfsa2021-14/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23994>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23995>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23998>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23961>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23999>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24002>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29945>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29946>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29948>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23996>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23997>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24000>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24001>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29947>