Alerta de seguridad cibernética	9VSA21-00379-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de enero de 2021
Última revisión	29 de enero 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, comparte la información entregada por Mozilla, sobre vulnerabilidades que afectan a Firefox, Firefox ESR y Thunderbird.

Este informe incluye las medidas de mitigación, consistentes en implementar medidas recomendadas por el proveedor e instalar las actualizaciones de los productos afectados cuando estén disponibles.

Vulnerabilidades

CVE-2021-23953
CVE-2021-23954
CVE-2021-23955
CVE-2021-23964
CVE-2021-23965

Impacto

Las siguientes son identificadas por Mozilla como vulnerabilidades de alto riesgo:

CVE-2021-23953 permite a un atacante elaborar un PDF especialmente diseñado, que al ser abierto por un usuario puede confundir al lector de PDF para que filtre información de origen cruzado.

CVE-2021-23954 permite a un atacante provocar una confusión de tipo de archivo que lleve a corrupción de memoria y un crash potencialmente explotable.

CVE-2021-23955 permite que el Firefox pueda ser confundido para transferir un estado de bloqueo del cursos a otra pestaña, lo que podría llevar a ataques de clickjacking.

CVE-2021-23964 y CVE-2021-23965 consisten en errores de seguridad de memoria, algunos de los cuales evidencian corrupción de memoria, por lo que desarrolladores de Mozilla estiman posible que podrían ser explotados para ejecutar código arbitrario.

Productos afectados

Mozilla Thunderbird, versiones anteriores a la 78.7.
Firefox ESR, versiones anteriores a la 78.7.
Firefox, versiones anteriores a la 85.

Mitigación

Instalar las correspondientes actualizaciones desde el sitio del proveedor.

Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/

https://www.mozilla.org/en-US/security/advisories/mfsa2021-04/

https://www.mozilla.org/en-US/security/advisories/mfsa2021-05/