

Alerta de seguridad cibernética	9VSA21-00374-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2021
Última revisión	25 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 Gentoo, sobre una vulnerabilidad que afecta a Mozilla Thunderbird.

Este informe incluye las medidas de mitigación, consistentes en instalar las últimas actualizaciones de los productos afectados.

## Vulnerabilidad

CVE-2020-16044

## Impacto

Las vulnerabilidades de riesgo alto son las siguientes:

CVE-2020-16044: Permite a un atacante remoto comprometer sistemas vulnerables debido a un error de uso de memoria después de ser liberada al procesar COOKIE-ECHO en un paquete SCTP.

### Productos afectados

Mozilla Thunderbird hasta la versión 78.6.1.

### Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

### Enlaces

<https://security.gentoo.org/glsa/202101-14>

<https://www.mozilla.org/en-US/security/advisories/mfsa2021-02/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16044>