

Alerta de seguridad cibernética	9VSA21-00353-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de enero de 2021
Última revisión	07 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 respecto a vulnerabilidad crítica que afecta a su explorador web Firefox y que podría permitir la ejecución de código arbitrario.

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

Vulnerabilidad

CVE-2020-16044

Impacto

Un par de atacantes podría modificar un fragmento de "COOKIE-ECHO" en un paquete SCTP de forma que se podría gatillar una vulnerabilidad de uso de memoria después de ser liberada. Firefox supone que con suficiente esfuerzo se podría haber explotado para ejecutar código arbitrario.

Productos Afectados

Firefox, Firefox ESR y Firefox para Android.

Mitigación

Actualizar a la versión 84.0.2 de Firefox, 78.6.1 de Firefox ESR o 84.1.3 de Firefox para Android.

Enlaces

<https://www.mozilla.org/en-US/security/advisories/mfsa2021-01/>

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