

Alerta de seguridad cibernética	9VSA20-00172-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de abril de 2020
Última revisión	04 de abril de 2020

## 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 referente a dos vulnerabilidades críticas que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

## VULNERABILIDADES

CVE-2020-6819  
CVE-2020-6820

## CVE-2020-6819

### Impacto

Debido a un error en memoria causado por una condición de carrera ejecutando el destructor “nsDocShell”, un atacante remoto podría crear un sitio web especialmente diseñado, engañar a la víctima para que lo visite y gatillar el error de uso de memoria luego de ser liberada, logrando la ejecución de código arbitrario en el sistema y comprometiéndole.

## CVE-2020-6820

### Impacto

Debido a un error en memoria causado por una condición de carrera al manejar “ReadableStream”, un atacante remoto podría crear un sitio web especialmente diseñado, engañar a la víctima para que lo visite y gatillar el error de uso de memoria luego de ser liberada, logrando la ejecución de código arbitrario en el sistema y comprometiéndole.

### Productos Afectados

Firefox desde la versión 60.0 hasta la versión 74.0.

Firefox ESR desde la versión 60.0 hasta la versión 60.9.0 y desde la versión 68.0 hasta la versión 68.6.0.

### Mitigación

Para Firefox, actualizar a la versión 74.0.1.

Para Firefox ESR, actualizar a la versión 68.6.1.

### Enlace

<https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6819>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6820>