

Alerta de seguridad informática	9VSA20-00229-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de junio de 2020
Última revisión	01 de junio 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 afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de Mozilla referente a vulnerabilidad que al explorador Mozilla Firefox para iOS. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-12404

CVE-2020-12404

La implementación del puente nativo a JavaScript requiere que se pase un token único, el cual garantiza que, código que no sea de aplicación, no pueda llamar a las funciones de puente. Un atacante remoto podría obtener este token a través de la descarga de archivos de un usuario, ya que este se encuentra expuesto durante ese proceso.

Productos Afectados

Todas las versiones de Mozilla Firefox para el sistema operativo iOS.

Mitigación

Actualizar a la versión 26 de Mozilla Firefox para iOS.

Enlaces

<https://www.mozilla.org/en-US/security/advisories/mfsa2020-19/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12404>