

Alerta de seguridad informática	9VSA-00044-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de agosto de 2019
Última revisión	05 de agosto de 2019

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 vulnerabilidades detectadas en Firefox, explorador para navegación en internet, junto a su respectiva actualización para mitigar el riesgo.

Vulnerabilidades

- CVE-2019-11751
- CVE-2019-11746
- CVE-2019-11744
- CVE-2019-11742
- CVE-2019-11736
- CVE-2019-11753
- CVE-2019-11752
- CVE-2019-9812
- CVE-2019-11741
- CVE-2019-11743
- CVE-2019-11748
- CVE-2019-11749
- CVE-2019-5849
- CVE-2019-11750
- CVE-2019-11737
- CVE-2019-11738
- CVE-2019-11747
- CVE-2019-11734
- CVE-2019-11735
- CVE-2019-11740

Impactos

- Ejecución de código malicioso vía consola de comandos
- Manipulación de archivos y escalada de privilegios
- Ataque UXSS a través de addons.mozilla.org y accounts.firefox.com
- Brecha de datos a través de WebRTC
- Liberación de datos a través de Skia Graphics
- Caída a través de una vulnerabilidad de Spidermonkey
- Aplicación de directorios CSP no aplicados correctamente
- Uso malicioso de JS saltando permisos de CSP
- Sitios removidos de la lista precargada de HSTS
- Corrupción de memoria con posibilidad de ejecución de código
- Más información sobre impactos de CVEs en informe 9VSA-00043-001

Productos Afectados

Mozilla Firefox: 66.0.2, 66.0.3, 66.0.4, 66.0.5, 67.0, 67.0.1, 67.0.2, 67.0.3, 67.0.4, 68.0, 68.0.1, 68.0.2

Mitigación

Actualizar a la versión de Firefox 69.

Enlace

- <https://www.mozilla.org/en-US/security/advisories/mfsa2019-25>
- <https://www.cybersecurity-help.cz/vdb/SB2019090305>