Alerta de Seguridad Informática

Alerta de seguridad informática	9VSA-00043-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de septiembre de 2019
Última revisión	03 de septiembre 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 vulnerabilidades detectadas en Firefox ESR, explorador para navegación en internet, junto con sus respectivas actualizaciones para mitigar el riesgo.

Vulnerabilidad

CVE-2019-11746

Impacto

La vulnerabilidad existe debido a un error "use-after-free". Un atacante remoto puede crear un sitio web especialmente diseñado, engañar a la víctima para que lo visite, activar un error de uso libre y ejecutar código arbitrario en el sistema de destino con privilegios del usuario actual. La explotación exitosa de la vulnerabilidad puede permitir a un atacante comprometer el sistema vulnerable

Productos Afectados

- Firefox ESR: 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 60.7.1, 60.7.2, 60.8.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Versión 60.9

Enlace

https://www .mozilla.org/en-US/security/advisories/mfsa2019-25/
https://www.cybersecurity-help.cz/vdb/SB2019090307

Vulnerabilidad

CVE-2019-11744

Impacto

Esta vulnerabilidad permite al atacante remoto realizar ataques XSS utilizando de manera Indebida los elementos title y textarea con innerHTML

Productos Afectados

- Firefox ESR: 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 60.7.1, 60.7.2, 60.8.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Versión 60.9

Enlace

https://www .mozilla.org/en-US/security/advisories/mfsa2019-25/
https://www.cybersecurity-help.cz/vdb/SB2019090307

Vulnerabilidad

CVE-2019-11742

Impacto

Esta vulnerabilidad permite al atacante obtener acceso a información sensible usando una combinación de filtros SVG y <canvas> element, debido a un error de la política “same-origin “, la cual se aplica al contenido de la imagen en caché.

Productos Afectados

- Firefox ESR: 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 60.7.1, 60.7.2, 60.8.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Versión 60.9

Enlace
https://www .mozilla.org/en-US/security/advisories/mfsa2019-25/
https://www.cybersecurity-help.cz/vdb/SB2019090307

Vulnerabilidad

CVE-2019-11753

Impacto

Esta vulnerabilidad permite al usuario escalar privilegios modificando durante la instalación de Firefox la ubicación del explorador en otros usuarios. El servicio de mantención de Mozilla no valida correctamente los privilegios de la ubicación y si se realiza una modificación durante esta, se puede lograr escalar privilegios. Nota: esta vulnerabilidad solo es aplicable en Windows, y se requiere acceso local al sistema.

Productos Afectados

- Firefox ESR: 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 60.7.1, 60.7.2, 60.8.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Versión 60.9

Enlace

https://www .mozilla.org/en-US/security/advisories/mfsa2019-25/
https://www.cybersecurity-help.cz/vdb/SB2019090307

Vulnerabilidad

CVE-2019-11752

Impacto

Esta vulnerabilidad existe debido a un error en el uso de memoria luego de su liberación al extraer un key value de IndexedDB. El atacante remoto podría usar una página especialmente diseñada para engañar a la víctima para que la visite, gatillar un error de “use-after-free” eliminado el valor y luego extrayéndolo durante la conversión. La explotación de esta vulnerabilidad permite al atacante comprometer al sistema afectado.

Productos Afectados

- Firefox ESR: 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 60.7.1, 60.7.2, 60.8.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Versión 60.9

Enlace

https://www .mozilla.org/en-US/security/advisories/mfsa2019-25/
https://www.cybersecurity-help.cz/vdb/SB2019090307

Vulnerabilidad

CVE-2019-9812

Impacto

Esta vulnerabilidad permite al atacante escapar de la Sandbox, utilizando la sincronización de Firefox, cargando accounts[.]firefox[.]com y forzando un log-in a una cuenta de sincronización maliciosa. Configuraciones de esta cuenta desactivarían al sandbox y serían cargadas en el explorador, el cual se reiniciaría sin esta opción.

Productos Afectados

- Firefox ESR: 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 60.7.1, 60.7.2, 60.8.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Versión 60.9

Enlace

https://www .mozilla.org/en-US/security/advisories/mfsa2019-25/
https://www.cybersecurity-help.cz/vdb/SB2019090307

Vulnerabilidad

CVE-2019-11743

Impacto

Esta vulnerabilidad permite al atacante obtener acceso a información sensible. La incorrecta implementación del evento “unload” podría permitir al atacante obtener acceso al historial de la víctima a través de una página modificada.

Productos Afectados

- Firefox ESR: 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 60.7.1, 60.7.2, 60.8.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Versión 60.9

Enlace

https://www.mozilla.org/en-US/security/advisories/mfsa2019-27/

Vulnerabilidad

CVE-2019-11740

Impacto

Desarrolladores de Mozilla y miembros de la comunidad descubrieron un error en la memoria el cual permite mostrar evidencia de memoria corrupta, y se presume que un atacante podría explotar esta vulnerabilidad con código malicioso. Un ataque exitoso podría permitir al atacante comprometer completamente al sistema.

Productos Afectados

- Firefox ESR: 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 60.7.1, 60.7.2, 60.8.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

- Versión 60.9
- Versión 68.1

Enlace

https://www .mozilla.org/en-US/security/advisories/mfsa2019-25/
https://www.cybersecurity-help.cz/vdb/SB2019090307

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.03 23:16:31 -04'00'