Alerta de seguridad cibernética	9VSA20-00204-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de mayo de 2020
Última revisión	06 de mayo 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 múltiples vulnerabilidades que afectan a sus exploradores Firefox y Firefox ESR. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-6831
CVE-2020-12387
CVE-2020-12388
CVE-2020-12389
CVE-2020-12390
CVE-2020-12391
CVE-2020-12392
CVE-2020-12393
CVE-2020-12394
CVE-2020-12395
CVE-2020-12396

CVE-2020-6831

Debido a un error en memoria al procesar fragmentos SCTP en WebRTC, un atacante remoto podría crear una página web especialmente diseñada para que una víctima acceda a esta, gatille el error en memoria y logre vulnerar al sistema del afectado, comprometiéndole completamente.

CVE-2020-12387

Debido a un error de uso de memoria luego de ser liberada, causado por una condición de carrera al ejecutar el código de apagado para "Web Worker", un atacante podría crear un sitio especialmente diseñado, para que una víctima lo visite, gatille el error en memoria y así logre comprometer completamente al sistema afectado.

CVE-2020-12388

Debido a que los procesos de contenidos de Firefox no bloqueaban de forma suficiente el control de acceso, debido a la protección inadecuada de los tokens de acceso, un atacante remoto podía evadir estas restricciones de seguridad y lograr la ejecución de código arbitrario en el sistema afectado.
Esta vulnerabilidad solo afecta a usuarios en Windows.

CVE-2020-12389

Debido a que los procesos de contenidos de Firefox no bloqueaban de forma suficiente el control de acceso para diferentes tipos de procesos, un atacante remoto podía evadir estas restricciones de seguridad y lograr la ejecución de código arbitrario en el sistema afectado.
Esta vulnerabilidad solo afecta a usuarios en Windows.

CVE-2020-12390

Debido a una incorrecta serialización de origen en "nslPrincipal origin" para direcciones IPv6, un atacante remoto podía evadir estas restricciones de seguridad a través de un enlace especialmente diseñado.

CVE-2020-12391

Debido a documentos construidos utilizando enlaces "*data:*" en un elemento "*object*" fallaban al heredar el CSP (Políticas de Seguridad de Contenido) del contexto de creación. Un atacante remoto podía ejecutar código arbitrario, el cual debería haber sido bloqueado, aunque con un origen opaco único.

CVE-2020-12392

Debido a que en las herramientas de desarrollador, en la pestaña "Network" la característica "Copy as Curl" no escapaba correctamente el método HTTP de una petición, la cual puede ser controlada por el sitio, si un usuario usaba esa característica y luego lo pegaba en la terminal, podía resultar en la inyección de comandos, y por ende, ejecución arbitraria de comandos, comprometiendo al sistema.

CVE-2020-12393

Debido a que en las herramientas de desarrollador, en la pestaña "Network" la característica "Copy as Curl" no escapaba correctamente los datos de una petición HTTP POST, la cual puede ser controlada por el sitio, si un usuario usaba esa característica y luego lo pegaba en la terminal, podía resultar en la filtración de archivos locales.
Esta vulnerabilidad solo afecta a usuarios en Windows.

CVE-2020-12394

Debido a una falencia lógica en barra de dirección, un usuario local podría suplantar la ubicación actual, seleccionando un origen diferente y eliminando el foco del elemento de entrada, logrando generar un ataque Spoofing.

CVE-2020-12395

Debido a un error en los límites de la memoria al procesar contenido HTML, un atacante remoto podría crear una página web especialmente diseñada para que una víctima acceda a esta, gatille el error en memoria y logre vulnerar al sistema del afectado, comprometiéndole completamente.

CVE-2020-12396

Debido a un error en los límites de la memoria al procesar contenido HTML, un atacante remoto podría crear una página web especialmente diseñada para que una víctima acceda a esta, gatille el error en memoria y logre vulnerar al sistema del afectado, comprometiéndole completamente.

Mitigación

Productos Afectados

Firefox desde la versión 60.0 hasta la 75.0.
Firefox ESR desde la versión 60.0 hasta la 68.7.0.

Mitigación

Para Firefox, actualizar a la versión 76.0.
Para Firefox ESR, actualizar a la versión 68.8.

Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2020-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-17/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6831
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12387
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12388
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12389
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12390
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12391
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12392
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12393
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12394
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12395
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12396

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.05.06 16:12:10 -04'00'