Alerta de seguridad cibernética	9VSA20-00298-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de septiembre de 2020
Última revisión	10 de septiembre 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 obtenida de Mozilla referente a múltiples vulnerabilidades que afectan a sus productos. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-15652
CVE-2020-6514
CVE-2020-15655
CVE-2020-15653
CVE-2020-6463
CVE-2020-15656
CVE-2020-15658
CVE-2020-15657
CVE-2020-15654
CVE-2020-15659
CVE-2020-15650
CVE-2020-15649
CVE-2020-15662
CVE-2020-15661
CVE-2020-15651

CVE-2020-15652: Al observar los rastros de la pila en busca de errores JavaScript en los “Web Workers”, es posible obtener el resultado de una redirección “Cross-origin”. Esto solo aplica a contenido que puede ser parseado como Script.
Impacto: Alto.

CVE-2020-6514: WebRTC usaba la dirección de memoria de la instancia de una clase como identificador de conexión. Este valor suele ser transmitido al par con quien se tiene la conexión, lo que permite la evasión de ASLR (Aleatoriedad en la disposición del espacio de direcciones.).
Impacto: Alto.

CVE-2020-15655: Una petición HTTP redirigida, la cual pueda ser observada o modificada a través de una extensión web, podría evadir los chequeos CORS, llevando a una potencial filtración de información del Cross-origin.
Impacto: Alto

CVE-2020-15653: Se descubrió que los “<iframe sandbox>” que tengan la flag “allow-popups” activada, podrían ser evadidos utilizando enlaces “noopener”. Esto podría llevar a problemas de seguridad para sitios que dependan de las configuraciones de Sandbox que permitan popus y y alojen contenido arbitrario.
Impacto: Medio.

CVE-2020-6463: Archivos media especialmente diseñados podrían llevar a una condición de carrera en caché de texturas (ANGLE gl::Texture::onUnbindAsSamplerTexture), resultando en el uso de memoria después de ser liberada, corrupción de memoria y un fallo potencialmente explotable.
Impacto: Medio.

CVE-2020-15656: Las optimizaciones en JIT que incluyen el objecto JavaScript “arguments” podrían confundir optimizaciones posteriores. El riesgo había sido mitigado con múltiples precauciones en el código, resultando en una vulnerabilidad nivel moderado.
Impacto: Medio.

CVE-2020-15658: El código para descargar archivos no tenía suficiente cuidado con caracteres especiales, lo cual permitía a un atacante cortar el final del archivo en una posición temprana, llevando a la descarga de tipos de archivos diferentes a los mostrados en el diálogo.
Impacto: Bajo.

CVE-2020-15657: Era posible cargar un archivo DLL en Firefox desde el directorio de instalación. Esto requería que el atacante lograra inyectar los archivos en el directorio previamente. Esta vulnerabilidad solo afecta a sistemas operativos Windows.
Impacto: Bajo.

CVE-2020-15654: En un ciclo infinito, un sitio especificando un puntero personalizado utilizando CSS podía hacer parecer que el usuario estaba interactuando con la página, cuando en realidad no era así.

Esto podía llevar a tener la percepción de estar viendo un fallo, especialmente cuando las interacciones con los diálogos del explorador no funcionan.
Impacto: Bajo.

CVE-2020-15659: Múltiples fallos en memoria descubiertos por desarrolladores y miembros de la comunidad de Mozilla, los cuales podían llevar a la corrupción de memoria y ejecución de código arbitrario.
Impacto: Alto.

Productos Afectados
Explorador web Mozilla Firefox.

Mitigaciones
Actualizar a la versión 79 de Firefox.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-30/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15652
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15655
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15653
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6463
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15656
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15658
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15657
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15654
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15659

MFSA-2020-31

CVE-2020-15652: Al observar los rastros de la pila en busca de errores JavaScript en los “Web Workers”, es posible obtener el resultado de una redirección “Cross-origin”. Esto solo aplica a contenido que puede ser parseado como Script.
Impacto: Alto.

CVE-2020-6514: WebRTC usaba la dirección de memoria de la instancia de una clase como identificador de conexión. Este valor suele ser transmitido al par con quien se tiene la conexión, lo que permite la evasión de ASLR (Aleatoriedad en la disposición del espacio de direcciones.).
Impacto: Alto.

CVE-2020-6463: Archivos media especialmente diseñados podrían llevar a una condición de carrera en caché de texturas (ANGLE gl::Texture::onUnbindAsSamplerTexture), resultando en el uso de memoria después de ser liberada, corrupción de memoria y un fallo potencialmente explotable.

Impacto: Medio.

CVE-2020-15650: Dada una aplicación de selección de archivos maliciosa, un atacante podría sobrescribir archivos locales y además, sobrescribir configuraciones de Firefox. (Pero no acceder al perfil anterior).
Impacto: Medio.

CVE-2020-15649: Dada una aplicación de selección de archivos maliciosa, un atacante podría robar y subir a internet archivos locales, sin importar cuales son elegidos para subir.
Impacto: Medio.

CVE-2020-15659: Múltiples fallos en memoria descubiertos por desarrolladores y miembros de la comunidad de Mozilla, los cuales podían llevar a la corrupción de memoria y ejecución de código arbitrario.
Impacto: Alto.

Productos Afectados
Mozilla Firefox ESR.

Mitigaciones
Actualizar a la versión 68.11 de Mozilla Firefox ESR.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-31/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15652
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6463
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15650
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15659

MFSA-2020-32

CVE-2020-15652: Al observar los rastros de la pila en busca de errores JavaScript en los “Web Workers”, es posible obtener el resultado de una redirección “Cross-origin”. Esto solo aplica a contenido que puede ser parseado como Script.
Impacto: Alto.

CVE-2020-6514: WebRTC usaba la dirección de memoria de la instancia de una clase como identificador de conexión. Este valor suele ser transmitido al par con quien se tiene la conexión, lo que permite la evasión de ASLR (Aleatoriedad en la disposición del espacio de direcciones.).
Impacto: Alto.

CVE-2020-15655: Una petición HTTP redirigida, la cual pueda ser observada o modificada a través de una extensión web, podría evadir los chequeos CORS, llevando a una potencial filtración de información del Cross-origin.
Impacto: Alto

CVE-2020-15653: Se descubrió que los “<iframe sandbox>” que tengan la flag “allow-popups” activada, podrían ser evadidos utilizando enlaces “noopener”. Esto podría llevar a problemas de seguridad para sitios que dependan de las configuraciones de Sandbox que permitan popus y y alojen contenido arbitrario.
Impacto: Medio.

CVE-2020-6463: Archivos media especialmente diseñados podrían llevar a una condición de carrera en caché de texturas (ANGLE gl::Texture::onUnbindAsSamplerTexture), resultando en el uso de memoria después de ser liberada, corrupción de memoria y un fallo potencialmente explotable.
Impacto: Medio.

CVE-2020-15656: Las optimizaciones en JIT que incluyen el objecto JavaScript “arguments” podrían confundir optimizaciones posteriores. El riesgo había sido mitigado con múltiples precauciones en el código, resultando en una vulnerabilidad nivel moderado.
Impacto: Medio.

CVE-2020-15658: El código para descargar archivos no tenía suficiente cuidado con caracteres especiales, lo cual permitía a un atacante cortar el final del archivo en una posición temprana, llevando a la descarga de tipos de archivos diferentes a los mostrados en el diálogo.
Impacto: Bajo.

CVE-2020-15657: Era posible cargar un archivo DLL en Firefox desde el directorio de instalación. Esto requería que el atacante lograra inyectar los archivos en el directorio previamente. Esta vulnerabilidad solo afecta a sistemas operativos Windows.
Impacto: Bajo.

CVE-2020-15654: En un ciclo infinito, un sitio especificando un puntero personalizado utilizando CSS podía hacer parecer que el usuario estaba interactuando con la página, cuando en realidad no era así. Esto podía llevar a tener la percepción de estar viendo un fallo, especialmente cuando las interacciones con los diálogos del explorador no funcionan.
Impacto: Bajo.

CVE-2020-15659: Múltiples fallos en memoria descubiertos por desarrolladores y miembros de la comunidad de Mozilla, los cuales podían llevar a la corrupción de memoria y ejecución de código arbitrario.
Impacto: Alto.

Productos Afectados

Mozilla Firefox ESR.

Mitigaciones
Actualizar a la versión 78.1 de Mozilla Firefox ESR.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-32/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15652
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15655
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15653
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6463
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15656
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15658
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15657
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15654
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15659

MFSA-2020-33

CVE-2020-15652: Al observar los rastros de la pila en busca de errores JavaScript en los “Web Workers”, es posible obtener el resultado de una redirección “Cross-origin”. Esto solo aplica a contenido que puede ser parseado como Script.
Impacto: Alto.

CVE-2020-6514: WebRTC usaba la dirección de memoria de la instancia de una clase como identificador de conexión. Este valor suele ser transmitido al par con quien se tiene la conexión, lo que permite la evasión de ASLR (Aleatoriedad en la disposición del espacio de direcciones.).
Impacto: Alto.

CVE-2020-15655: Una petición HTTP redirigida, la cual pueda ser observada o modificada a través de una extensión web, podría evadir los chequeos CORS, llevando a una potencial filtración de información del Cross-origin.
Impacto: Alto

CVE-2020-15653: Se descubrió que los “<iframe sandbox>” que tengan la flag “allow-popups” activada, podrían ser evadidos utilizando enlaces “noopener”. Esto podría llevar a problemas de seguridad para sitios que dependan de las configuraciones de Sandbox que permitan popus y y alojen contenido arbitrario.
Impacto: Medio.

CVE-2020-6463: Archivos media especialmente diseñados podrían llevar a una condición de carrera en caché de texturas (ANGLE gl::Texture::onUnbindAsSamplerTexture), resultando en el uso de memoria después de ser liberada, corrupción de memoria y un fallo potencialmente explotable.
Impacto: Medio.

CVE-2020-15656: Las optimizaciones en JIT que incluyen el objecto JavaScript “arguments” podrían confundir optimizaciones posteriores. El riesgo había sido mitigado con múltiples precauciones en el código, resultando en una vulnerabilidad nivel moderado.
Impacto: Medio.

CVE-2020-15658: El código para descargar archivos no tenía suficiente cuidado con caracteres especiales, lo cual permitía a un atacante cortar el final del archivo en una posición temprana, llevando a la descarga de tipos de archivos diferentes a los mostrados en el diálogo.
Impacto: Bajo.

CVE-2020-15657: Era posible cargar un archivo DLL en Firefox desde el directorio de instalación. Esto requería que el atacante lograra inyectar los archivos en el directorio previamente. Esta vulnerabilidad solo afecta a sistemas operativos Windows.
Impacto: Bajo.

CVE-2020-15654: En un ciclo infinito, un sitio especificando un puntero personalizado utilizando CSS podía hacer parecer que el usuario estaba interactuando con la página, cuando en realidad no era así. Esto podía llevar a tener la percepción de estar viendo un fallo, especialmente cuando las interacciones con los diálogos del explorador no funcionan.
Impacto: Bajo.

CVE-2020-15659: Múltiples fallos en memoria descubiertos por desarrolladores y miembros de la comunidad de Mozilla, los cuales podían llevar a la corrupción de memoria y ejecución de código arbitrario.
Impacto: Alto.

Productos Afectados
Mozilla Thunderbird.

Mitigaciones
Actualizar a la versión 78.1 de Mozilla Thunderbird.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-33/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15652
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15655
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15653
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6463
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15656
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15658
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15657
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15654
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15659

CVE-2020-15662: Una página web fraudulenta podría anular el “WKUserScript” inyectado, utilizado por la funcionalidad de descarga. Esta explotación podría provocar que el usuario descargue archivos no deseados.
Impacto: Alto.

CVE-2020-15661: Una página web fraudulenta podría anular el “WKUserScript” inyectado, utilizado por el “autocompletar” de inicio de sesión. Esta explotación podría provocar que las claves utilizadas por los dominios actuales sean filtradas.
Impacto: Alto.

CVE-2020-15651: Se puede usar un carácter de orden RTL Unicode en el nombre del archivo descargado para cambiar el nombre del archivo durante el flujo de la Interfaz de Usuario de descarga para cambiar la extensión del archivo.
Impacto: Bajo.

Productos Afectados
Mozilla Firefox para iOS.

Mitigaciones
Actualizar a la versión 28 de Mozilla Firefox para iOS.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-34/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15662
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15661
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15651