Alerta de seguridad cibernética	9VSA20-00275-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de julio de 2020
Última revisión	18 de julio 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 respecto a múltiples vulnerabilidades que afectan a sus productos Firefox Mozilla y Thunderbird. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-15648
CVE-2020-12415
CVE-2020-12416
CVE-2020-12417
CVE-2020-12418
CVE-2020-12419
CVE-2020-12420
CVE-2020-12402
CVE-2020-12421
CVE-2020-12422
CVE-2020-12423
CVE-2020-12424
CVE-2020-12425
CVE-2020-12426

MSFA-2020-28

CVE-2020-15648: Utilizando objetos y etiquetas embebidas, era posible llamar a otros sitios aún si esto no era permitido por el encabezado “X-Frame-Option”.
Impacto: moderado.

Productos Afectados
Mozilla Firefox versiones 78 y anteriores.

Mitigaciones
Actualizar a la versión 78.0.2 de Mozilla Firefox.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-28/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15648

MSFA-2020-29

CVE-2020-12415: Envenenamiento del manifiesto AppCache debido al procesamiento de URL codificada
Cuando la cadena de caracteres “%2F” estaba presente en una URL de manifiesto, comportamiento confuso del AppCache de Firefox permitía a un manifiesto ser servido desde un subdirectorio, esto podría permitir al appcache ser utilizado para servir peticiones para un directorio de más alto nivel.
Impacto: alto

CVE-2020-12416: Uso de memoria luego de ser liberada en “WebRTC Video Broadcaster”
“VideoStreamEncoder” podía ser liberado en una condición de carrera con “VideoBroadcaster::AddOrUpdateSink”, resultando en un error de uso de memoria luego de ser liberada y un fallo potencialmente explotable.
Impacto: alto

CVE-2020-12417: Corrupción en memoria debido a signo de extensión ausente para “ValueTags” en ARM64
Debido a una confusión sobre “ValueTags” en objetos JavaScript, un objeto podría ser pasado a través la barrera de tipo, resultando en la corrupción de memoria y un fallo potencialmente explotable.
Impacto: alto

CVE-2020-12418: Filtración de información debido a objeto URL manipulado
Manipular partes individuales de un objeto URL podría causar la lectura fuera de los límites en memoria, filtrando memoria de procesos a JavaScript malicioso.
Impacto: alto

CVE-2020-12419: Uso de memoria luego de ser liberada en “nsGlobalWindowInner”
Al procesar funciones “Callbacks” que ocurrieron durante la renovación de ventana del proceso padre, la ventana asociada podría fallar, causando una condición de uso de memoria luego de ser liberada.
Impacto: alto

CVE-2020-12420: Uso de memoria luego de ser liberada al intentar conectarse a un servidor “STUN”
Al intentar conectarse a un servidor “STUN”, una condición de carrera podría causar el uso de memoria luego de ser liberada de un puntero, llevando a la corrupción de memoria y un fallo potencialmente explotable.
Impacto: alto

CVE-2020-15648: Utilizando objetos y etiquetas embebidas, era posible llamar a otros sitios aún si esto no era permitido por el encabezado “X-Frame-Option”.
Impacto: Moderado.

CVE-2020-12402: Generación de llave RSA vulnerable a ataque de canal lateral
Durante la generación de llave RSA, implementaciones “bignum” usan una variación del algoritmo “Binary Extended Euclidean”, que implicaba un flujo significativamente dependiendo de la entrada de datos. Esto podría permitir a un atacante realizar ataques de canal lateral basados en electromagnetismo para grabar rastros que lleven a la recuperación de claves primarias.
Impacto: moderado

CVE-2020-12421: Las actualizaciones de extensiones no respetaban las mismas reglas del certificado de confianza que las actualizaciones de software
Al realizar actualizaciones de extensiones, cadenas de certificados que terminen en “no creadas en la raíz” eran rechazadas, a pesar de haber sido legítimamente agregadas por un administrador. Esto llevaba a que algunas extensiones de usuarios no se actualicen y tampoco alerten sobre eso.
Impacto: moderado

CVE-2020-12422: Desbordamiento de un entero en “nsJPEGEncoder::emptyOutputBuffer”
En configuraciones no por defecto, una imagen JPEG creada por JavaScript podría causar que una variable interna de desborde, resultando en escritura fuera de los límites, corrupción en memoria y un fallo potencialmente explotable.
Impacto: moderado

CVE-2020-12423: Suplantación de archivo DLL al buscar “%PATH%” por una librería
Si el archivo DLL de Windows “webauthn.dll” no estaba, y en su lugar, se pusiera un archivo malicioso en el “%PATH%” del usuario, Firefox cargaría ese archivo, llevando a la ejecución de código.
Impacto: moderado

CVE-2020-12424: Se podría evadir la ventana de permisos de “WebRTC” por un proceso de contenido comprometido

Al construir una ventana de permisos en “WebRTC”, una URI es otorgada en el proceso de contenido. La URI no era confiable y podía utilizarse una URI que ya obtuvo permisos antes para evadir la ventana de permisos.
Impacto: bajo

CVE-2020-12425: Lectura fuera de los límites en memoria en “Data.parse()”
Debido a una confusión al procesar el carácter guion (–) en “Data.parse()”, era posible salirse un byte de los límites en memoria, permitiendo la lectura fuera de ella y la filtración de información.
Impacto: bajo

CVE-2020-12426: Vulnerabilidades de seguridad en memoria
Errores en memoria que con suficiente esfuerzo podrían llevar a la ejecución de código arbitrario en el sistema afectado.
Impacto: alto

Productos Afectados
Mozilla Thunderbird versiones anteriores a la 78.

Mitigaciones
Actualizar a la versión 78 de Mozilla Thunderbird.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-29/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15648
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12415
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12416
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12417
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12418
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12419
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12420
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15648
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12402
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12421
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12422
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12423
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12424
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12425
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12426