| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00323-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de noviembre de 2020 |
| Última revisión | 19 de noviembre 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 Mozilla respecto a múltiples vulnerabilidades que afectan al explorador web Mozilla Firefox y al cliente de correo Thunderbird. El presente informe incluye las respectivas medidas de mitigación.

## Vulnerabilidades

CVE-2020-26951
CVE-2020-26952
CVE-2020-16012
CVE-2020-26953
CVE-2020-26954
CVE-2020-26955
CVE-2020-26956
CVE-2020-26957
CVE-2020-26958
CVE-2020-26959
CVE-2020-26960
CVE-2020-15999
CVE-2020-26961
CVE-2020-26962
CVE-2020-26963
CVE-2020-26964
CVE-2020-26965
CVE-2020-26966
CVE-2020-26967
CVE-2020-26968
CVE-2020-26969

CVE-2020-26951: Una discrepancia entre la carga de evento y el formato en el código SVG de Firefox podría haber permitido que se activaran los eventos de carga, aun después de la sanitización. Un atacante que sea capaz de explotar una vulnerabilidad XSS en páginas internas privilegiadas, podría usar este ataque para evadir el sanitizador integrado.
Impacto: Alto

CVE-2020-26952: El recuento incorrecto de las funciones en línea durante la compilacion JIT, podría haber llevado a la corrupción de memoria y a un fallo potencialmente explotable al manejar errores de sin-memoria.
Impacto: Alto

CVE-2020-16012: Al dibujar una imagen transparente sobre una imagen de origen cruzado desconocida, la función "drawImage" de la librería gráfica Skia se tomaba un tiempo variable dependiendo del contexto de la imagen de abajo. El resultado podía ser una potencial exposición de información de origen cruzado del contenido de la imagen a través de un ataque de canal lateral cronometrado.
Impacto: Moderado

CVE-2020-26953: Era posible causar que el explorador entrara en modo pantalla completa sin mostrar la interfaz de usuario de seguridad, haciendo posible realizar ataques phishing o confundir al usuario.
Impacto: Moderado

CVE-2020-26954: Al aceptar un intent malicioso de otras aplicaciones instaladas, Firefox para Android aceptaba manifiestos de rutas de archivo arbitrarias y permitía declarar manifiestos de aplicaciones web para otros orígenes. Esto podía ser usado para obtener acceso al modo pantalla completa para suplantar la interfaz de usuario, y también podía llevar a ataques de origen cruzado en sitios objetivos. Nota: Esta vulnerabilidad solamente afecta al sistema operativo Android.
Impacto: Moderado

CVE-2020-26955: Cuando un usuario descarga un archivo en Firefox para Android, si se deja una cookie, esta iba a es reenviada durante la operación de descarga del archivo subsecuente en el mismo dominio, independiente de si la descarga original o subsecuente eran hechas en modo privado o no del explorador. Nota: Esta vulnerabilidad solamente afecta al sistema operativo Android.
Impacto: Moderado

CVE-2020-26956: En algunos casos, remover elementos HTML durante la sanitización podía mantener la existencia de manejadores de eventos SVG, los cuales podían llevar a ataques Cross-site Scripting (XSS) a través de la función pegar (manual y API portapapeles).
Impacto: Moderado

CVE-2020-26957: "OneCRL" no era funcional en el nuevo Firefox par aAndroid debido a la ausencia de un servicio de inicialización. Esto podía resultar en una falla en hacer cumplir la revocación de algunos certificados. Nota: Esta vulnerabilidad solamente afecta al sistema operativo Android.
Impacto: Moderado

CVE-2020-26958: Firefox no bloqueaba la ejecución de scripts con tipos MIME incorrectos cuando la respuesta era interceptada y cacheada a través de un "ServiceWorker". Esto podía llevar a la inclusión de una vulnerabilidad Cross-site Scripting (XSS) o una evasión de la política de seguridad de contenidos (CSP).
Impacto: Moderado

CVE-2020-26959: Durante la apagada del explorador, la decrementación de referencia podría haber sucedido en un objeto previamente liberado, resultando en el uso de memoria después de ser liberada, corrupción de memoria y un fallo potencialmente explotable.
Impacto: Moderado

CVE-2020-26960: Si el método "Compact()" era llamado en un "nsTArray", el arreglo podría haber sido realocado sin actualizar otros punteros, llevando a un potencial uso de memoria después de ser liberada y un fallo explotable.
Impacto: Moderado

CVE-2020-15999: En Freetype, si las imágenes PNG eran embebidas en fuentes, la función "Load_SBit_Png" contendía un desbordamiento de entero que llevaba a un desbordamiento del buffer en la pila, corrupción de memoria y un fallo potencialmente explotable. Nota: Solamente afecta a Linux y Android, y las condiciones para explotar la vulnerabilidad son difíciles.
Impacto: Moderado

CVE-2020-26961: Cuando se utiliza DNS en el protocolo HTTPs, intencionalmente se filtran rangos de IP RFC1918 y relacionados de las respuestas, ya que no tiene sentido que vengan de un resolutor DoH. Sin embargo, cuando una dirección IPv4 era mapeada a través de IPv6, las direcciones eran erróneamente permitidas, llevando a un potencial ataque de reencuentro de DNS.
Impacto: Moderado

CVE-2020-26962: Elementos "iframe" de origen cruzado que contenían formularios de conexión podrían haber sido reconocidos por el servicio de autocompletado, rellenando con las credenciales. Esto podría haber llevado a posibles ataques clickjacking, como también leerse en particiones de asilamiento primario dinámico asolado.
Impacto: Bajo

CVE-2020-26963: Repetidas llamadas a las interfaces de historial y ubicación podrían haber sido usadas para dejar colgado al explorador. Esta vulnerabilidad fue arreglada introduciendo un límite de llamada a las APIs.
Impacto: Bajo

CVE-2020-26964:
Si la función de debugging remoto vía USB estaba habilitada en Firefox para Android en una versión de Android menor a la 6.0, aplicaciones no confiables podrían haberse conectado a la función para operar bajo los privilegios del explorador y leer e interactuar con los contenidos web. La característica fue implementada como un socket de dominio Unix, protegida por la política Android SELinux; sin embargo, SELinux no era enforzado en versiones anteriores a la 6.0. Nota: Esta vulnerabilidad solo afecta a Firefox para Android.
Impacto: Bajo

CVE-2020-26965: Algunos sitios tienen la característica "Mostrar contraseña" en donde al pinchar un botón, el campo contraseña se cambiará a texto plano, revelando la contraseña escrita. Si, al usar un programa de teclado que recuerde datos ingresados, el usuario escribe su contraseña y luego aprieta en mostrar contraseña, el campo era cambiado a texto plano, resultando en la posibilidad de que la aplicación de teclado recuerde la contraseña aun cuando fue escrita bajo el tipo de campo "contraseña".
Impacto: Bajo

CVE-2020-26966: Realizar una búsqueda de una sola palabra en la barra de direcciones causaba el envío una petición mDNS a través de la red local, en busca del hostname que tenga esa palabra, resultando en una filtración de información. Nota: Esta vulnerabilidad solo afecta al sistema operativo Windows.
Impacto: Bajo

CVE-2020-26967: Al estar a la escucha por cambios en la página con "Mutation Observer", una página web maliciosa podría confundir a las capturas de pantalla de Firefox para que interactúen con otros elementos además que los que fueron inyectados en el sitio. Esto podría llevar a errores internos y comportamientos no esperados en el código de las capturas de pantalla.
Impacto: Bajo

CVE-2020-26968: Errores en memoria encontrados en Firefox y Firefox ESR. Algunos de estos mostraban evidencia de corrupción de memoria, y Mozilla presume que con algún esfuerzo estas vulnerabilidades podrían haber sido explotadas para la ejecución de código remoto.
Impacto: Alto.

CVE-2020-26969: Errores en memoria encontrados en Firefox. Algunos de estos mostraban evidencia de corrupción de memoria, y Mozilla presume que con algún esfuerzo estas vulnerabilidades podrían haber sido explotadas para la ejecución de código remoto.
Impacto: Alto.

## Productos Afectados
La vulnerabilidad afecta al explorador web Firefox Mozilla versiones anteriores a la 83.

## Mitigación

La vulnerabilidad fue mitigada en la versión 83 de Firefox Mozilla.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-50/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26952
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26954
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26955
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26957
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15999
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26968
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26969

## MFSA-2020-51

CVE-2020-26951: Una discrepancia entre la carga de evento y el formato en el código SVG de Firefox podría haber permitido que se activaran los eventos de carga, aun después de la sanitización. Un atacante que sea capaz de explotar una vulnerabilidad XSS en páginas internas privilegiadas, podría usar este ataque para evadir el sanitizador integrado.
Impacto: Alto

CVE-2020-16012: Al dibujar una imagen transparente sobre una imagen de origen cruzado desconocida, la función "drawImage" de la librería gráfica Skia se tomaba un tiempo variable dependiendo del contexto de la imagen de abajo. El resultado podía ser una potencial exposición de información de origen cruzado del contenido de la imagen a través de un ataque de canal lateral cronometrado.
Impacto: Moderado

CVE-2020-26953: Era posible causar que el explorador entrara en modo pantalla completa sin mostrar la interfaz de usuario de seguridad, haciendo posible realizar ataques phishing o confundir al usuario.

Impacto: Moderado

CVE-2020-26956: En algunos casos, remover elementos HTML durante la sanitización podía mantener la existencia de manejadores de eventos SVG, los cuales podían llevar a ataques Cross-site Scripting (XSS) a través de la función pegar (manual y API portapapeles).
Impacto: Moderado

CVE-2020-26958: Firefox no bloqueaba la ejecución de scripts con tipos MIME incorrectos cuando la respuesta era interceptada y cacheada a través de un "ServiceWorker". Esto podía llevar a la inclusión de una vulnerabilidad Cross-site Scripting (XSS) o una evasión de la política de seguridad de contenidos (CSP).
Impacto: Moderado

CVE-2020-26959: Durante la apagada del explorador, la decrementación de referencia podría haber sucedido en un objeto previamente liberado, resultando en el uso de memoria después de ser liberada, corrupción de memoria y un fallo potencialmente explotable.
Impacto: Moderado

CVE-2020-26960: Si el método "Compact()" era llamado en un "nsTArray", el arreglo podría haber sido realocado sin actualizar otros punteros, llevando a un potencial uso de memoria después de ser liberada y un fallo explotable.
Impacto: Moderado

CVE-2020-15999: En Freetype, si las imágenes PNG eran embebidas en fuentes, la función "Load_SBit_Png" contendía un desbordamiento de entero que llevaba a un desbordamiento del buffer en la pila, corrupción de memoria y un fallo potencialmente explotable. Nota: Solamente afecta a Linux y Android, y las condiciones para explotar la vulnerabilidad son difíciles.
Impacto: Moderado

CVE-2020-26961: Cuando se utiliza DNS en el protocolo HTTPs, intencionalmente se filtran rangos de IP RFC1918 y relacionados de las respuestas, ya que no tiene sentido que vengan de un resolutor DoH. Sin embargo, cuando una dirección IPv4 era mapeada a través de IPv6, las direcciones eran erróneamente permitidas, llevando a un potencial ataque de reencuentro de DNS.
Impacto: Moderado

CVE-2020-26965: Algunos sitios tienen la característica "Mostrar contraseña" en donde al pinchar un botón, el campo contraseña se cambiará a texto plano, revelando la contraseña escrita. Si, al usar un programa de teclado que recuerde datos ingresados, el usuario escribe su contraseña y luego aprieta en mostrar contraseña, el campo era cambiado a texto plano, resultando en la posibilidad de que la aplicación de teclado recuerde la contraseña aun cuando fue escrita bajo el tipo de campo "contraseña".
Impacto: Bajo

CVE-2020-26966: Realizar una búsqueda de una sola palabra en la barra de direcciones causaba el envío una petición mDNS a través de la red local, en busca del hostname que tenga esa palabra,

resultando en una filtración de información. Nota: Esta vulnerabilidad solo afecta al sistema operativo Windows.
Impacto: Bajo

CVE-2020-26968: Errores en memoria encontrados en Firefox y Firefox ESR. Algunos de estos mostraban evidencia de corrupción de memoria, y Mozilla presume que con algún esfuerzo estas vulnerabilidades podrían haber sido explotadas para la ejecución de código remoto.
Impacto: Alto.

### Productos Afectados
La vulnerabilidad afecta al explorador web Firefox Mozilla ESR versiones anteriores a la 78.5.

### Mitigación
La vulnerabilidad fue mitigada en la versión 78.5 de Firefox Mozilla ESR.

### Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-51/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15999
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26968

## MFSA-2020-52

CVE-2020-26951: Una discrepancia entre la carga de evento y el formato en el código SVG de Thunderbird podría haber permitido que se activaran los eventos de carga, aun después de la sanitización. Un atacante que sea capaz de explotar una vulnerabilidad XSS en páginas internas privilegiadas, podría usar este ataque para evadir el sanitizador integrado.
Impacto: Alto

CVE-2020-16012: Al dibujar una imagen transparente sobre una imagen de origen cruzado desconocida, la función "drawImage" de la librería gráfica Skia se tomaba un tiempo variable dependiendo del contexto de la imagen de abajo. El resultado podía ser una potencial exposición de información de origen cruzado del contenido de la imagen a través de un ataque de canal lateral cronometrado.
Impacto: Moderado

CVE-2020-26953: Era posible causar que el explorador entrara en modo pantalla completa sin mostrar la interfaz de usuario de seguridad, haciendo posible realizar ataques phishing o confundir al usuario.
Impacto: Moderado

CVE-2020-26956: En algunos casos, remover elementos HTML durante la sanitización podía mantener la existencia de manejadores de eventos SVG, los cuales podían llevar a ataques Cross-site Scripting (XSS) a través de la función pegar (manual y API portapapeles).
Impacto: Moderado

CVE-2020-26958: Thuderbird no bloqueaba la ejecución de scripts con tipos MIME incorrectos cuando la respuesta era interceptada y cacheada a través de un "ServiceWorker". Esto podía llevar a la inclusión de una vulnerabilidad Cross-site Scripting (XSS) o una evasión de la política de seguridad de contenidos (CSP).
Impacto: Moderado

CVE-2020-26959: Durante la apagada del explorador, la decrementación de referencia podría haber sucedido en un objeto previamente liberado, resultando en el uso de memoria después de ser liberada, corrupción de memoria y un fallo potencialmente explotable.
Impacto: Moderado

CVE-2020-26960: Si el método "Compact()" era llamado en un "nsTArray", el arreglo podría haber sido realocado sin actualizar otros punteros, llevando a un potencial uso de memoria después de ser liberada y un fallo explotable.
Impacto: Moderado

CVE-2020-15999: En Freetype, si las imágenes PNG eran embebidas en fuentes, la función "Load_SBit_Png" contendía un desbordamiento de entero que llevaba a un desbordamiento del buffer en la pila, corrupción de memoria y un fallo potencialmente explotable. Nota: Solamente afecta a Linux y Android, y las condiciones para explotar la vulnerabilidad son difíciles.
Impacto: Moderado

CVE-2020-26961: Cuando se utiliza DNS en el protocolo HTTPs, intencionalmente se filtran rangos de IP RFC1918 y relacionados de las respuestas, ya que no tiene sentido que vengan de un resolutor DoH. Sin embargo, cuando una dirección IPv4 era mapeada a través de IPv6, las direcciones eran erróneamente permitidas, llevando a un potencial ataque de reencuentro de DNS.
Impacto: Moderado

CVE-2020-26965: Algunos sitios tienen la característica "Mostrar contraseña" en donde al pinchar un botón, el campo contraseña se cambiará a texto plano, revelando la contraseña escrita. Si, al usar un programa de teclado que recuerde datos ingresados, el usuario escribe su contraseña y luego aprieta en mostrar contraseña, el campo era cambiado a texto plano, resultando en la posibilidad de que la aplicación de teclado recuerde la contraseña aun cuando fue escrita bajo el tipo de campo "contraseña".

Impacto: Bajo

CVE-2020-26966: Realizar una búsqueda de una sola palabra en la barra de direcciones causaba el envío una petición mDNS a través de la red local, en busca del hostname que tenga esa palabra, resultando en una filtración de información. Nota: Esta vulnerabilidad solo afecta al sistema operativo Windows.
Impacto: Bajo

CVE-2020-26968: Errores en memoria encontrados en Mozilla Thunderbird. Algunos de estos mostraban evidencia de corrupción de memoria, y Mozilla presume que con algún esfuerzo estas vulnerabilidades podrían haber sido explotadas para la ejecución de código remoto.
Impacto: Alto.

## Productos Afectados

La vulnerabilidad afecta al cliente de correo Mozilla Thunderbird versiones anteriores a la 78.5.

## Mitigación

La vulnerabilidad fue mitigada en la versión 78.5 de Mozilla Thunderbird.

## Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2020-52/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15999
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26968