Alerta de seguridad informática	9VSA20-00114-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de enero de 2020
Última revisión	09 de enero 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 información obtenida de Mozilla, referente a vulnerabilidades que afectan a sus exploradores Firefox y Firefox ESR, las cuales de ser explotadas, permitirían a un atacante remoto obtener información confidencial, inyectar código de forma remota, saltar ciertas restricciones de seguridad, entre otras cosas. En el contenido de este informe se encuentra la respectiva mitigación.

Vulnerabilidades

CVE-2019-17016
CVE-2019-17017
CVE-2019-17018
CVE-2019-17019
CVE-2019-17015
CVE-2019-17020
CVE-2019-17021
CVE-2019-17022
CVE-2019-17023
CVE-2019-17024
CVE-2019-17025

Impacto

CVE-2019-17016
Esta vulnerabilidad permitiría a un atacante remoto acceder a información sensible debido a la débil sanitización de datos de entrada que se realiza cuando se copia un tag desde el clipboard hacia un editor de texto rico, el sanitizador CSS reescribe incorrectamente una regla @namespace, lo cual permite la inyección en ciertos tipos de sitios resultando en la filtración de datos.

CVE-2019-17017
Debido a un error de confusión de tipo al procesar contenido HTML en XPCVariant.cpp, un atacante remoto podría crear una página web especialmente diseñada, gatillar el error de confusión de tipo y ejecutar código arbitrario en el sistema víctima, comprometiendo completamente al sistema vulnerable.

CVE-2019-17018
Al abrir el explorador en modo privado en Windows 10, el teclado en pantalla retendría las palabras de sugerencias para mejorar la precisión del teclado, permitiendo a un usuario local acceder a esta información utilizada durante el modo privado.

CVE-2019-17019
Esta vulnerabilidad permitiría a un atacante remoto ejecutar código arbitrario en el sistema afectado debido a na incorrecta forma de procesar scripts en Python. Cuando Python es instalado en Windows, al seleccionar abrir desde el módulo de descargas en el explorador, el archivo Python que utilice el MIME de tipo text/plain podría ser ejecutado por Python en vez de ser abierto como archivo de texto.

CVE-2019-17015
Esta vulnerabilidad existe debido a un error con los límites de memoria durante la inicialización de un nuevo proceso de contenido. Un atacante remoto podría crear un sitio web especialmente diseñado, para que la víctima, al acceder a éste, gatille la corrupción de memoria y ejecute código arbitrario en el sistema de la víctima, comprometiéndolo completamente. Esta vulnerabilidad solo afecta a Windows.

CVE-2019-17020
Debido a la incorrecta implementación del CSP (Content Security Policy) que no es impuesta por las hojas de estilo XSL aplicadas a documentos XML, si éstas incluyen por ejemplo, JavaScript, podría saltarse cualquier restricción del CSP en el documento XML, permitiendo a un atacante remoto realizar acciones maliciosas en el sistema.

CVE-2019-17021
Esta vulnerabilidad existe debido a una condición de carrera de procesos que ocurre durante la inicialización de un nuevo proceso de contenido. Un atacante remoto podría explotar esta condición ganando acceso a información potencialmente sensible, como la dirección de pila del proceso padre. Esta vulnerabilidad afecta solamente a Windows.

CVE-2019-17022
Debido a la insuficiente sanitización de datos entregados por el usuario dentro del sanitizador CSS, cuando se copia un tag desde el clipboard hacia un editor de texto rico, el sanitizador no maneja correctamente los caracteres "<" y ">". Si posteriormente un sitio web copia el innerHTML del noto y lo asigna a otro innerHTML, esto provocaría una vulnerabilidad XSS (Cross-site Scripting).

CVE-2019-17023
Esta vulnerabilidad se debe a la negociación insegura después del "HelloRetryRquest" en Mozilla NSS, que puede llevar a elegir un protocolo menos seguro (por ejemplo TLS 1.2 o menor) luego de que "HelloRetryRequest" TLS 1.3 es enviado.

CVE-2019-17024, CVE-2019-17025
Esta vulnerabilidad existe debido a un error con los límites de memoria al procesar contenido HTML. Un atacante remoto podría crear un sitio especialmente diseñado, engañar a una víctima a entrar en él, gatillar la corrupción de memoria y ejecutar código arbitrario en el sistema, comprometiéndole completamente.

Productos Afectados

Todas las versiones de Firefox entre la 66.0 hasta la 71.0. (Para el CVE-2019-17022 sólo entre la 70.0 hasta la 71.0).
Todas las versiones de Firefox ERS entre la 60.0 hasta la 68.30.

Mitigación
Se deben aplicar las actualizaciones de seguridad publicadas por Mozilla publicadas en los enlaces al final del documento.
Para Firefox se debe actualizar a la versión 72.
Para Firefox ERS se debe actualizar a la versión 68.4.

Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2020-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-02/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17024
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17025

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.09 16:05:26 -03'00'