Alerta de seguridad informática	9VSA20-00119-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2020
Última revisión	13 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 Mozilla Thunderbird, 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. Este informe incluye la respectiva mitigación.

Vulnerabilidad

CVE-2019-17015

CVE-2019-17016

CVE-2019-17017

CVE-2019-17021

CVE-2019-17022

CVE-2019-17024

CVE-2019-17026

Impacto

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 cuando la víctima acceda 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-2019-17016

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-2019-17021

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-2019-17024

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.

CVE-2019-17026
Debido a un error de confusión de tipo con los componentes StoreElementHole y FallibleStoreElement al procesar contenido HTML en el compilador IonMonkey JIT, un atacante remoto podría crear una página web especialmente diseñada, engañar a la víctima para que acceda a éste, gatillar el error de confusión de tipo y ejecutar código arbitrario en el sistema víctima, comprometiendo completamente al sistema vulnerable. Este fallo está siendo explotado actualmente y se considera crítico, por lo que se recomienda actualizar urgentemente a la última versión de Firefox.

Productos Afectados
Todas las versiones de Mozilla Thunderbird desde la 60.0 hasta la 68.3.1.

Mitigación
Se debe actualizar a la versión 68.4.1 de Mozilla Thunderbird.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-04/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17015
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-2019-17021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17024
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17026