Alerta de seguridad cibernética	9VSA20-00207-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de mayo de 2020
Última revisión	08 de mayo 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 entregada por Mozilla referente a múltiples vulnerabilidades que afectan al cliente de correo Mozilla Thunderbird. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-6831
CVE-2020-12387
CVE-2020-12392
CVE-2020-12393
CVE-2020-12395
CVE-2020-12397

CVE-2020-6831

Debido a un error en memoria al procesar fragmentos SCTP en WebRTC, un atacante remoto podría crear una página web especialmente diseñada para que una víctima acceda a esta, gatille el error en memoria y logre vulnerar al sistema del afectado, comprometiéndole completamente.

CVE-2020-12387

Debido a un error de uso de memoria luego de ser liberada, causado por una condición de carrera al ejecutar el código de apagado para "Web Worker", un atacante podría crear un sitio especialmente diseñado, para que una víctima lo visite, gatille el error en memoria y así logre comprometer completamente al sistema afectado.

CVE-2020-12392

Debido a que en las herramientas de desarrollador, en la pestaña "Network" la característica "Copy as Curl" no escapaba correctamente el método HTTP de una petición, la cual puede ser controlada por el sitio, si un usuario usaba esa característica y luego lo pegaba en la terminal, podía resultar en la inyección de comandos, y por ende, ejecución arbitraria de comandos, comprometiendo al sistema.

CVE-2020-12393

Debido a que en las herramientas de desarrollador, en la pestaña "Network" la característica "Copy as Curl" no escapaba correctamente los datos de una petición HTTP POST, la cual puede ser controlada por el sitio, si un usuario usaba esa característica y luego lo pegaba en la terminal, podía resultar en la filtración de archivos locales.
Esta vulnerabilidad solo afecta a usuarios en Windows.

CVE-2020-12395

Debido a un error en los límites de la memoria al procesar contenido HTML, un atacante remoto podría crear una página web especialmente diseñada para que una víctima acceda a esta, gatille el error en memoria y logre vulnerar al sistema del afectado, comprometiéndole completamente.

CVE-2020-12397

Debido al incorrecto procesamiento de dirección de correo emisoras, un atacante remoto podría suplantar la dirección email utilizando caracteres Unicode codificados y así, engañar a una víctima haciéndola pensar que recibió un correo de otro usuario.

Productos Afectados

Mozilla Thunderbird desde la versión 60.0 hasta la 60.9.1. y desde la versión 68.0 hasta la 68.7.

Mitigación

Actualizar a la versión 68.8 de Mozilla Thunderbird.

Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2020-18/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6831
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12387
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12392
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12393
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12395
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12397

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.05.08 18:55:58 -04'00'