| | |
|---|---|
| Alerta de seguridad informática | 9VSA20-00140-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de febrero de 2020 |
| Última revisión | 13 de febrero 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 múltiples vulnerabilidades que afectan a cliente de correo Mozilla Thunderbird. De ser explotadas, estas permitirían a un atacante causar denegación de servicios, obtener información sensible y hasta comprometer completamente al sistema vulnerable. Este informe incluye la respectiva mitigación.

## Vulnerabilidades

CVE-2020-6792

CVE-2020-6793

CVE-2020-6794

CVE-2020-6795

CVE-2020-6797

CVE-2020-6798

CVE-2020-6800

## Impactos

CVE-2020-6792
Debido a un error en el proceso de cálculo de ID del mensaje que utiliza datos sin inicializar en adición al contenido de los mensajes, un atacante podría explotar esta vulnerabilidad y obtener acceso a información potencialmente sensible.

CVE-2020-6793
Un atacante podría enviar un email especialmente diseñado a la víctima causando un error de lectura fuera de los límites de memoria, lo cual le permitiría obtener información potencialmente sensible y causar una denegación de servicios en la aplicación.

CVE-2020-6794
Debido a un error en la funcionalidad de gestión de contraseñas al utilizar la contraseña maestra que fue actualizada después de Thunderbird 60. La contraseña antigua todavía se encontraba disponible en el sistema, sin encriptar. Un atacante podría obtener información sensible explotando esta vulnerabilidad.

CVE-2020-6795
Debido a un error de desreferencia en el puntero NULL al procesar mensajes con múltiples firmas S/MIME, un atacante podría enviar correos especialmente diseñados para causar una denegación de servicios en la aplicación de la víctima.

CVE-2020-6797
Debido a un error de acceso indebido con extensiones que tienen permitido realizar descargas, un atacante podría saltarse restricciones de seguridad y abrir o ejecutar aplicaciones arbitrarias en el sistema de la víctima. Esta vulnerabilidad solo afecta a usuarios de Mac OSX.

CVE-2020-6798
Por causa de una deficiente validación de datos ingresados al manejar tags de templates, un atacante podría confundir al parser de JavaScript enviando peticiones especialmente diseñadas y ejecutando código arbitrario sobre el sistema de la víctima. La explotación de esta vulnerabilidad le permitiría al atacante comprometer completamente al sistema afectado.

CVE-2020-6800
Por causa de un error de memoria al procesar contenido HTML, un atacante podría crear un sitio especialmente diseñado, engañar a la víctima para que acceda a este y causar una corrupción de memoria permitiéndole ejecutar código arbitrario en el sistema de la víctima y comprometiéndolo completamente.

## Productos Afectados

Mozilla Thunderbird desde la versión 60.0 hasta la 60.9.1, y desde la versión 68.0 hasta la 68.4.2.
(El CVE-2020-6794 también afecta desde la versión 52.0 hasta la 52.9.0).

## Mitigación

Actualizar a la versión 68.5 de Mozilla Thunderbird.

## Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2020-07/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6792
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6793
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6794
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6795
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6798
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6800

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.13 19:27:53 -03'00'