Alerta de seguridad informática	9VSA20-00155-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de marzo de 2020
Última revisión	13 de marzo 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 comprometer completamente al sistema afectado. Este informe incluye su respectiva mitigación.

Vulnerabilidades

CVE-2020-6805

CVE-2020-6806

CVE-2020-6807

CVE-2020-6811

CVE-2020-6812

CVE-2020-6814

CVE-2019-20503

Impactos

CVE-2020-6805

Debido a un error de uso de memoria después de ser liberada (use-after-free) al eliminar datos sobre orígenes en el gestor de Quota. Un atacante remoto podría crear una página especialmente diseñada para que cuando una víctima la visite, se genere el error en memoria, logrando la ejecución de código remoto y comprometiendo al sistema.

CVE-2020-6806

Debido a un error de lectura fuera de los límites de memoria (out-of-bounds read) provocado por la falta de protección en contra de la confusión de estados en “BodyStream::OnInputStreamReady”, un atacante podría engañar a una víctima para que visite una página especialmente diseñada, gatillar el error en memoria y finalmente obtener la ejecución de código remoto en el sistema vulnerable, comprometiéndole completamente.

CVE-2020-6807

Debido a un error de uso de memoria luego de ser liberada (use-after-free) en “cubeb” durante la destrucción de la transmisión, un atacante podría engañar a una víctima para que visite una página especialmente diseñada, gatillar el error en memoria y finalmente obtener la ejecución de código remoto en el sistema vulnerable, comprometiéndole completamente.

CVE-2020-6811

Debido a la insuficiente validación de datos ingresados por el usuario al utilizar la característica “Copy as cURL” en la pestaña de red en las herramientas de desarrollador, un atacante podría engañar a una víctima para que copie datos maliciosos y luego los inserte en la consola del sistema operativo. Una explotación exitosa resultaría en la ejecución de comandos de OS por parte de la víctima engañada.

CVE-2020-6812

Cuando se conectan “AirPods” a un iPhone por primera vez, estos obtienen el nombre del dueño por defecto, (por ejemplo, Claudia’s AirPods). Sitios web con permisos de cámara web o micrófono pueden enumerar dispositivos, obteniendo así los nombres de dispositivos cercanos (información que debiese ser privada).

CVE-2020-6814
Debido a un error de memoria (buffer overflow) al procesar contenido HTML, un atacante remoto podría crear un sitio especialmente diseñado para que cuando la víctima lo visite, se gatille el error en memoria, permitiendo al atacante realizar la ejecución de código remoto sobre el sistema afectado y comprometiéndole completamente.

CVE-2019-20503
Debido a un error de lectura fuera de los límites de memoria (out-of-bounds read) en "sctp_load_addresses_from_init", un atacante podría entregarle datos especialmente diseñados a la aplicación para gatillar el error en memoria y así acceder a datos en memoria del sistema vulnerable.

Producto Afectado
Mozilla Thunderbird desde la versión 60.0 hasta la 60.9 y desde la versión 68.0 hasta la 68.5.

Mitigación
Se debe aplicar la actualización de seguridad 68.6 publicada por Mozilla, la cual se encuentra en los enlaces al final del documento.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-10/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6805
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6806
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6807
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6811
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6812
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6814
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20503

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.13 12:32:57 -03'00'