Alerta de seguridad cibernética	9VSA20-00234-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de junio de 2020
Última revisión	04 de junio 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 obtenida de Mozilla referente a múltiples vulnerabilidades que afectan su cliente de correo Thunderbird. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2020-12399
CVE-2020-12405
CVE-2020-12406
CVE-2020-12410
CVE-2020-12398

CVE-2020-12398

La vulnerabilidad existe en el uso de "STARTTLS" en un servidor IMAP cuando se envía una respuesta PREAUTH. En dicho caso, Thunderbird continuará con una conexión sin cifrar, lo que hará que los datos de correo electrónico se envíen sin protección y puedas ser robados por un atacante.

CVE-2020-12399

Debido a que las firmas DSA muestran diferencias de tiempos en NSS, un atacante remoto podría aprovecharse de esta vulnerabilidad para robar las claves privadas.

CVE-2020-12405

Debido a un error de uso de memoria después de ser liberada, por causa de una condición de carrera en el componente "SharedWorkerService", un atacante remoto podría crear un sitio web especialmente diseñado, engañar a una víctima para que la abra, gatillar el error en memoria y ejecutar código arbitrario en el sistema afectado.

CVE-2020-12406

Debido a un error de confusión de tipos durante la eliminación de objetos JavaScript empaquetados. Un atacante remoto podría crear una página web especialmente diseñada, engañar a la víctima para que la abra, activar el error de confusión de tipo y ejecutar código arbitrario en el sistema afectado.

CVE-2020-12410

Debido a un error en los límites de la memoria al procesar contenido HTML. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la abra, gatillar el error en memoria y ejecutar código arbitrario en el sistema afectado. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso total del sistema vulnerable.

Productos Afectados
Mozilla Thunderbird entre las versiones 60.0 y 68.8.1.

Mitigación
Actualizar a la versión 68.9.0 de Mozilla Thunderbird.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2020-22/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12398
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12399
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12405
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12406
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12410