Alerta de seguridad informática	9VSA20-00154-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de marzo de 2020
Última revisión	11 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 sus exploradores Firefox y Firefox ESR, 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-2020-6808

CVE-2020-6809

CVE-2020-6810

CVE-2020-6811

CVE-2020-6812

CVE-2020-6813

CVE-2020-6814

CVE-2020-6815

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-2020-6808

Por causa de un incorrecto procesamiento de datos ingresados por el usuario, un atacante podría un sitio y utilizar funciones JavaScript para suplantar la dirección URL, permitiéndole al atacante suplantar sitios web.

CVE-2020-6809

Un atacante podría acceder a datos sensibles del sistema de la víctima si es que esta instala un plugin web malicioso. Esto debido a una insuficiente gestión de permisos y controles de acceso a archivos locales.

CVE-2020-6810

Es posible realizar un ataque de suplantación debido a que el explorador, luego de ingresar al modo pantalla completa, puede ocultar la notificación que indica que el navegador esta en este modo, esto por causa de ventanas emergentes anteriores. Esto podría llevar a confundir al usuario sobre el origen actual de la página permitiendo a un atacante robar credenciales u otros datos.

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-2020-6813
Esta vulnerabilidad permite a un atacante remoto evitar ciertas restricciones de seguridad, esto debido a que al proteger bloques CSS con la función "nonce" de la Política de Seguridad de Contenido, la declaración "@import" en el bloque CSS podría permitir que un atacante inyecte estilos arbitrarios, evitando la Política de seguridad de contenido.

CVE-2020-6814, CVE-2020-6815
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.

Productos Afectados
Para Firefox, desde la versión 73.0.1 hacia atrás.
Para Firefox ESR, desde la versión 68.5.0 hacia atrás.

Mitigación

Se deben aplicar las actualizaciones de seguridad publicadas por Mozilla publicadas en los enlaces al final del documento.
Para Firefox se debe actualizar a la versión 74.
Para Firefox ERS se debe actualizar a la versión 68.6.

Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2020-08/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-09/
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-2020-6808
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6809
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6810
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-2020-6813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6814
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6815
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20503

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.11 16:09:18 -03'00'