Alerta de seguridad informática	9VSA-00096-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de diciembre de 2019
Última revisión	5 de diciembre de 2019

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 del sitio oficial de Mozilla referente a vulnerabilidades que afectan a Firefox y Firefox ESR, las cuales, de ser explotadas, pueden resultar en ataques de denegación de servicios, corrupción de datos y ejecución de código remoto, las que son consideradas como críticas. El informe incluye las respectivas actualizaciones para mitigar los riesgos asociados.

Vulnerabilidades

CVE-2019-11745
CVE-2019-11756
CVE-2019-13722
CVE-2019-17005
CVE-2019-17008
CVE-2019-17009
CVE-2019-17010
CVE-2019-17011
CVE-2019-17012
CVE-2019-17013
CVE-2019-17014

Impactos

CVE-2019-11745: Al utilizar un cifrado de bloque, si se realiza una llamada a NSC_EncryptUpdate con datos más pequeños que el tamaño del bloque, podría producirse una escritura fuera de los límites de la memoria. Esto podría corromper la pila en la memoria y botar la aplicación, causando una denegación de servicios potencialmente explotable.

CVE-2019-11756: Esta vulnerabilidad sólo aplica para Firefox. Debido a un recuento incorrecto de los tokens de sesión, se podría provocar un escape en la memoria, el cual podría botar la aplicación, causando una denegación de servicios.

CVE-2019-13722: Esta vulnerabilidad sólo aplica en Windows. Al otorgar un nombre de hilo en WebRTC, es posible entregar un valor incorrecto de argumentos, llevando a la corrupción de la pila en la memoria para causar una denegación de servicios potencialmente explotable.

CVE-2019-17005: El serializador de texto plano utiliza un arreglo de tamaño fijo para la cantidad de elementos que podría procesar, sin embargo, es posible desbordar este arreglo lo cual llevaría a la corrupción de memoria y podría botar la aplicación, causando una denegación de servicios potencialmente explotable.

CVE-2019-17008: Esta vulnerabilidad sólo aplica para Firefox ESR. Es posible causar una denegación de servicios potencialmente explotable al eliminar “workers” cuando se trabaja con “nested workers”.

CVE-2019-17009: Esta vulnerabilidad sólo aplica para Windows, y solo puede ser explotada de forma local. El servicio de actualización, al estar ejecutándose, realiza escritura de status y archivos log a una locación sin restringir, lo cual potencialmente permitiría a un proceso sin privilegios localizar y explotar esta vulnerabilidad de manejo de archivos en el servicio de actualización.

CVE-2019-17010: Bajo ciertas condiciones, al revisar las preferencias de “Resist Fingerprinting” durante las revisiones de orientación del dispositivo, una condición de carrera en procesamiento podría causar un escape en la memoria, causando una denegación de servicios potencialmente explotable.

CVE-2019-17011: Bajo ciertas condiciones, al retirar un documento desde un DocShell en el código de anti-seguimiento, una condición de carrera en procesamiento podría causar un escape en la memoria, causando una denegación de servicios potencialmente explotable.

CVE-2019-17012: Se encontraron vulnerabilidades en Firefox 70 y Firefox ESR 68.2, las cuales mostraban evidencia de corrupción en memoria y se presume que podrían haber sido explotadas para causar ejecución de código arbitrario.

CVE-2019-17013: Esta vulnerabilidad sólo aplica para Firefox. Se encontraron vulnerabilidades, las cuales mostraban evidencia de corrupción en memoria se presume que podrían haber sido explotadas para causar ejecución de código arbitrario.

CVE-2019-17014: Esta vulnerabilidad sólo aplica para Firefox. Si una imagen no ha sido cargada correctamente (como cuando se intenta subir otro tipo de archivo en vez de una imagen), ésta podría arrastrarse y soltarse entre dominios, provocando una fuga de información de origen cruzado.

Productos Afectados
Todas las versiones de Firefox anteriores a la 71 son vulnerables.
Todas las versiones de Firefox ESR anteriores a la 68.3 son vulnerabl

Mitigaciones
Actualizar a la versión 71 de Firefox.
Actualizar a la versión 68.3 de Firefox ESR.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2019-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-37/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11745
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11756
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13722
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17005
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17008
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17009
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17010
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17011
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17012
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17013
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17014

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.05 17:21:33 -03'00'