Alerta de seguridad informática	9VSA20-00139-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Febrero de 2020
Última revisión	12 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 sus exploradores de internet, la cuales de ser explotadas, permitirían a un atacante comprometer completamente al sistema vulnerable. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2020-6796
CVE-2020-6797
CVE-2020-6798
CVE-2020-6799
CVE-2020-6800
CVE-2020-6801

Impactos

CVE-2020-6796

Debido a un error durante la lectura de memoria compartida en procesos padre, un atacante podría enviarle a la víctima un sitio web especialmente diseñado para corromper la memoria, ejecutando código arbitrario sobre el sistema de la víctima. La explotación de esta vulnerabilidad le permitiría al atacante comprometer completamente al sistema afectado.

CVE-2020-6797

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-2020-6799

Debido a una deficiente validación de datos al abrir enlaces de PDFs desde otras aplicaciones (con Firefox configurado para abrir este tipo de extensiones), un atacante remoto podría enviar enlaces especialmente diseñados a la víctima para ejecutar comandos de sistema operativo arbitrarios en el sistema de la víctima. Esta vulnerabilidad solo afecta al sistema operativo Windows y si es que se utiliza Firefox como la aplicación predeterminada para abrir extensiones no-predeterminadas.

CVE-2020-6800, CVE-2020-6801

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 Firefox desde la versión 61.0 hasta la versión 72.0.2.
Mozilla Firefox ESR desde la versión 60.0 hasta la 60.9.0 y desde la versión 68.0 hasta la 68.4.2

Mitigación

Para Mozilla Firefox, actualizar a la versión 73.
Para Mozilla Firefox ESR, actualizar a la versión 68.5.

Enlaces

https:/www.mozilla.org/en-US/security/advisories/mfsa2020-06/
https:/www.mozilla.org/en-US/security/advisories/mfsa2020-05/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6796
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-2020-6799
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6800
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6801

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.12 17:57:41 -03'00'