| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00173-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 07 de abril de 2020 |
| Última revisión | 07 de abril 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 entregada por Mozilla referente a múltiples vulnerabilidades críticas que afectan a sus navegadores Firefox y Firefox ESR. El presente informe incluye las respectivas medidas de mitigación.

## VULNERABILIDADES

CVE-2020-6821
CVE-2020-6822
CVE-2020-6823
CVE-2020-6824
CVE-2020-6825
CVE-2020-6826
CVE-2020-6827
CVE-2020-6828

## CVE-2020-6821

### Impacto
Debido a un error en memoria al utilizar el método WebGL “copyTextSubImage”, un atacante remoto podría engañar a una víctima para que acceda a un sitio especialmente diseñado, gatillar el error de lectura fuera de los límites de la memoria y leer contenidos de sin inicializar en el sistema afectado.

### Productos Afectados
Firefox desde la versión 60.0 hasta la versión 74.0.1.
Firefox ESR desde la versión 60.0 hasta la versión 60.9.0 y desde la versión 68.0 hasta la versión 68.6.1.

## CVE-2020-6822

### Impacto
Debido a un error en memoria en “GMPDecodeData” al procesar imágenes más grandes que 4Gb en arquitecturas 32-bit, un atacante remoto podría crear una imagen especialmente diseñada, engañar a una víctima para que la abra y gatillar el error de escritura fuera de los límites de la memoria, logrando ejecutar código arbitrario y permitiéndole comprometer al sistema afectado.

### Productos Afectados
Firefox desde la versión 60.0 hasta la versión 74.0.1.
Firefox ESR desde la versión 60.0 hasta la versión 60.9.0 y desde la versión 68.0 hasta la versión 68.6.1.

## CVE-2020-6823

### Impacto
Debido a incorrecto manejo de permisos de extensiones, una extensión maliciosa podría llamar a “browser.identity.launchWebAuthFlow”, controlando el “redirect_uri” y a través del valor retornado, obtener el código “Auth”, comprometiendo completamente la cuenta del usuario en el navegador.

### Productos Afectados
Firefox desde la versión 60.0 hasta la versión 74.0.1.

## CVE-2020-6824

### Impacto
Debido a un incorrecto funcionamiento del generador de claves en modo privado, si un usuario crea su clave en él y luego cierra la ventana, sin cerrar el explorador, un atacante podría abrir otra sesión privada, visitar el mismo sitio y Firefox generará una idéntica.

### Productos Afectados
Firefox desde la versión 60.0 hasta la versión 74.0.1.

## CVE-2020-6825

### Impacto
Debido a un error en memoria al procesar contenido HTML, un atacante remoto podría engañar a una víctima para que acceda a un sitio especialmente diseñado, gatillar el error de corrupción de memoria y ejecutar código arbitrario, comprometiendo al sistema vulnerable.

### Productos Afectados
Firefox desde la versión 60.0 hasta la versión 74.0.1.
Firefox ESR desde la versión 60.0 hasta la versión 60.9.0 y desde la versión 68.0 hasta la versión 68.6.1.

## CVE-2020-6826

### Impacto
Debido a un error en memoria al procesar contenido HTML, un atacante remoto podría engañar a una víctima para que acceda a un sitio especialmente diseñado, gatillar el error de corrupción de memoria y ejecutar código arbitrario, comprometiendo al sistema vulnerable.

### Productos Afectados
Firefox desde la versión 60.0 hasta la versión 74.0.1.

## CVE-2020-6827

### Impacto
Debido al incorrecto procesamiento de la URL “intent://-schemed”, un atacante remoto podría engañar a Firefox para Android para que muestre una URI incorrecta.
Esta vulnerabilidad solo afecta a Android.

### Productos Afectados
Firefox ESR desde la versión 60.0 hasta la versión 60.9.0 y desde la versión 68.0 hasta la versión 68.6.1.

# CVE-2020-6828

### Impacto
Una aplicación Android maliciosa podría crear un “Intent”, el cual, al ser procesado por Firefox, podría resultar en la sobreescritura de archivos en el directorio de perfil del usuario. Una forma de explotar esta vulnerabilidad sería entregarle a “user.js” valores maliciosos arbitrarios, permitiendo comprometer al sistema afectado.
Esta vulnerabilidad solo afecta a Android.

### Productos Afectados
Firefox ESR desde la versión 60.0 hasta la versión 60.9.0 y desde la versión 68.0 hasta la versión 68.6.1.

# MITIGACIÓN

### Mitigación
Para Firefox, actualizar a la versión 74.0.2.
Para Firefox ESR, actualizar a la versión 68.6.2.

### Enlace
https://www.mozilla.org/en-US/security/advisories/mfsa2020-12/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-13/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6821
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6822
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6823
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6826
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6828

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.07 15:03:49 -04'00'