10/04/2022

Alerta de Seguridad Digital

[TLP: WHITE]
[PAP: WHITE]

Actualizaciones Disponibles Corrección Vulnerabilidades en Firefox

Debido a las últimas vulnerabilidades de seguridad halladas en Firefox, los desarrolladores de Mozilla han puesto a disposición de la comunidad la última versión **Firefox 99,** las cuales corrigen estas vulnerabilidades. A continuación, se listan las vulnerabilidades de seguridad y que son mitigadas cuando el usuario instala esta última versión.

Vulnerabilidad	Producto afectado	Descripción	Impacto
CVE-2022-1097 y *CVE-2022-28282*	Firefox	Da lugar a vulnerabilidad de tipo UAF (*user-after-free*), en donde se hace un uso incorrecto de la memoria dinámica, un ciberdelincuente puede aprovechar esta vulnerabilidad para piratear el programa.	**Alto**
CVE-2022-28281		Da lugar a vulnerabilidad de tipo *Out-of-bounds write*, en donde el puntero incrementa o reduce mas allá de los límites de la memoria, lo cual produce bloqueo y ejecución de código arbitrario.	**Alto**
CVE-2022-28283		La función *sourceMapURL* posee una vulnerabilidad en donde se pueden incluir archivos locales	**Moderado**

		confidenciales en un sitio web.	
CVE-2022-28284		El elemento de SVG se puede usar para cargar contenido como scripts ejecutables.	**Moderado**
CVE-2022-28285		Permite lectura de memoria fuera de los límites.	**Moderado**
CVE-2022-28286		Visualización de contenido *IFRAME* que conllevan a de suplantación de identidad.	**Bajo**
CVE-2022-24713		Provoca denegación de servicio en el navegador debido a vulnerabilidad en expresiones regulares.	**Bajo**
CVE-2022-28289		Error de límite en la memoria cuando proceso contenido HTML, un ciberdelincuente puede diseñar un sitio web manipulado y ejecutar código arbitrario en el sistema cuando el usuario haga clic en el sitio phishing.	**Alto**
CVE-2022-28288		Errores de seguridad en memoria presentes en versión 98 y que dan lugar a la ejecución de código malicioso.	**Moderado**

Tabla No. 1. *Vulnerabilidades mitigadas por versión 99 en Firefox [1].*

Pese a que no existe aún un exploit público en donde se ejecuten dichas vulnerabilidades, se pide a las entidades públicas privadas y a la comunidad en general actualizar con la última versión el navegador Firefox.

Para realizar la debida actualización en su navegador Firefox, se deben realizar los siguientes pasos: Diríjase al botón ubicado en la parte superior derecha demarcado con este símbolo ☰, seguidamente haga clic en **ayuda** o **Help** y **About Firefox.**

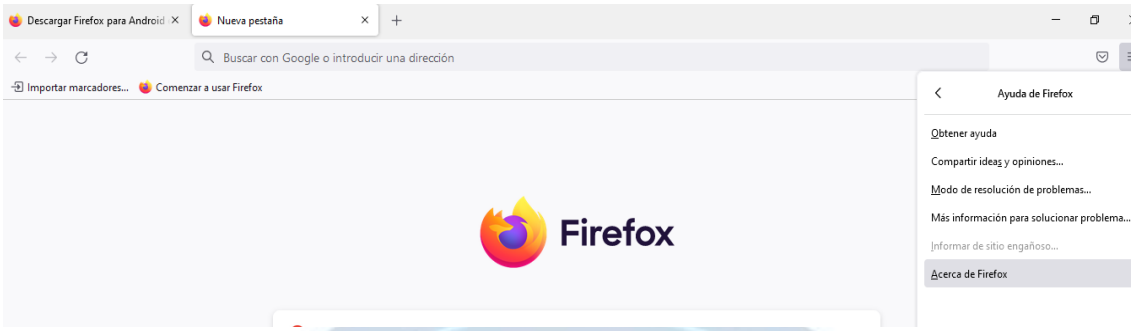

Figura No. 1. Acerca de Firefox.

Y luego de dar clic, se abre la descarga de las ultimas actualizaciones del sistema, como se muestra a continuación.

Figura No. 2. *Actualización de Firefox.*

Figura No 3. *Actualización de Firefox a versión 99.*

Luego de terminada la descarga, proceda a reiniciar el navegador para poner en marcha la nueva versión.

Recomendaciones:

- Mantenga su navegador actualizado con la última versión liberada, realice los pasos de la figura 1 a la 3 para mantenerse al día con los parches de Firefox.
- Descargar Firefox desde el sitio oficial, siempre comprobando la URL.
- Mantenga actualizado y parchado su sistema operativo.
- Mantenga actualizado su solución de antivirus.
- Realice copias de respaldo de su información.

Referencias:

[1] Mozilla Security, "Security Vulnerabilities fixed in Firefox 99" [Online] https://www.mozilla.org/en-US/security/advisories/mfsa2022-13/#CVE-2022-28283
https://www.mozilla.org/en-US/firefox/99.0/releasenotes/

Canales de Atención

Si tiene alguna consulta técnica, puede comunicarse con el CSIRT Gobierno de tratarse de una entidad del Estado, o con el ColCERT si pertenece a cualquier otro sector de la economía, a través de los siguientes canales:

Bogotá: +57 601 344 22 22
Línea Gratuita Nacional: 018000952525 Opción 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT