	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°227	Fecha: 26-09-2023
		Página: 10 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Mozilla Firefox y Firefox ESR		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

Se han reportado múltiples vulnerabilidades de severidad **ALTA** de tipo escritura fuera de límites, uso después de la liberación y desbordamiento de búfer en Mozilla Firefox y Firefox ESR. La explotación exitosa de estas vulnerabilidades permite que un atacante remoto comprometa el sistema vulnerable.

2. **DETALLES:**

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5168, de tipo escritura fuera de límites, existe debido a un error de límite al procesar entradas que no son de confianza en FilterNodeD2D1. Un atacante remoto puede crear un sitio web especialmente diseñado, engañar a la víctima para que lo abra, provocar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5169, de tipo escritura fuera de límites, existe debido a un error de límite al procesar entradas que no son de confianza en PathOps. Un atacante remoto puede crear un sitio web especialmente diseñado, engañar a la víctima para que lo abra, provocar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5171, de tipo uso después de la liberación, existe debido a un error de uso después de la liberación durante la compilación de Ion. Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, provocar un error de uso posterior a la liberación y ejecutar código arbitrario en el sistema.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5176, de tipo desbordamiento de búfer, existe debido a un error de límite al procesar contenido HTML. Un atacante remoto puede crear un sitio web especialmente diseñado, engañar a la víctima para que lo abra, provocar daños en la memoria y ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5172, de tipo uso después de la liberación, existe debido a un error de uso después de la liberación en Ion Engine. Un atacante remoto puede engañar a la víctima para que abra una página web especialmente diseñada, provocar un error de uso después de la liberación y ejecutar código arbitrario en el sistema.

A. Productos afectados:

- Mozilla Firefox: 100.0 - 117.0.1 y 116.0 – 117.0.1.
- Firefox ESR: 102.0 - 115.2.1.
- Firefox para Android: 100.1.0 - 117.1.0 y 116.0 – 117.1.0.

3. **RECOMENDACIONES:**

- Actualizar el producto afectado a la última versión disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://www.mozilla.org/en-US/security/advisories/mfsa2023-42/ • hxxp://www.mozilla.org/en-US/security/advisories/mfsa2023-41/