

	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°254</b>		<b>Fecha: 24-10-2023</b>
	<b>Página: 7 de 15</b>		
Componente que reporta	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
Nombre de la alerta	Múltiples vulnerabilidades en Mozilla Firefox		
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		
<b>Descripción</b>			
<p><b>1. ANTECEDENTES:</b></p> <p>Se han reportado múltiples vulnerabilidades de severidad <b>ALTA</b> de tipo desbordamiento de búfer, omisión de funciones de seguridad y ataque de suplantación de identidad en Mozilla Firefox. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino, eludir las restricciones de seguridad implementadas y realizar un ataque de suplantación de identidad.</p> <p><b>2. DETALLES:</b></p> <p>Las vulnerabilidades de severidad <b>ALTA</b>, identificadas por MITRE como CVE-2023-5731 y CVE-2023-5730 de tipo desbordamiento del 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.</p> <p>La vulnerabilidad de severidad <b>ALTA</b>, identificada por MITRE como CVE-2023-5728 de tipo desbordamiento de búfer, existe debido a un seguimiento inadecuado de objetos durante la recolección de basura. 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.</p> <p>La vulnerabilidad de severidad <b>MEDIA</b>, identificada por MITRE como CVE-2023-5727 de tipo omisión de funciones de seguridad, existe debido a una advertencia de archivo ejecutable faltante al descargar archivos. msix, msixbundle, .appx y .appxbundle. Un atacante remoto puede engañar a la víctima para que ejecute los archivos y comprometer el sistema afectado.</p> <p>La vulnerabilidad de severidad <b>MEDIA</b>, identificada por MITRE como CVE-2023-5732 de tipo ataque de suplantación de identidad, existe debido al procesamiento incorrecto de los datos proporcionados por el usuario al manejar caracteres bidireccionales. Un atacante remoto puede falsificar la barra de direcciones del navegador.</p> <p>La vulnerabilidad de severidad <b>MEDIA</b>, identificada por MITRE como CVE-2023-5721 de tipo ataque de suplantación de identidad, existe debido a un procesamiento incorrecto del renderizado en cola. Un atacante remoto puede realizar un ataque de suplantación de identidad activando o descartando ciertos mensajes y cuadros de diálogo del navegador.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>– Mozilla Firefox: 100.0 - 118.0.2.</li> <li>– Firefox ESR: 102.0 - 115.3.1.</li> <li>– Firefox para Android: 100.1.0 - 118.2.0.</li> </ul> <p><b>3. RECOMENDACIÓN:</b></p> <ul style="list-style-type: none"> <li>• Actualizar los productos afectados a la última versión de software disponible que aborda estas vulnerabilidades.</li> </ul>			
Fuente de Información:	<ul style="list-style-type: none"> <li>• <a href="https://www.mozilla.org/en-US/security/advisories/mfsa2023-46/">hxxp://www.mozilla.org/en-US/security/advisories/mfsa2023-46/</a></li> <li>• <a href="https://www.mozilla.org/en-US/security/advisories/mfsa2023-45/">hxxp://www.mozilla.org/en-US/security/advisories/mfsa2023-45/</a></li> </ul>		