

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°011			Fecha: 12-01-2024
				Página: 7 de 12
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA			
Nombre de la alerta	Múltiples vulnerabilidades en Microsoft Edge			
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				
<p>1. ANTECEDENTES:</p> <p>Se ha reportado múltiples vulnerabilidades de severidad ALTA y MEDIA de tipo error de validación de entrada, permisos, privilegios y controles de acceso y omisión de funciones de seguridad en Microsoft Edge. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto comprometer el sistema afectado, eludir las restricciones de seguridad, realizar un ataque de denegación de servicio (DoS) y ejecutar código arbitrario en el sistema de destino.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta, identificada por MITRE como CVE-2024-20709 de tipo error de validación de entrada, existe debido a una validación insuficiente de la entrada proporcionada por el usuario al analizar JavaScript dentro de archivos PDF. Un atacante remoto puede engañar a la víctima para que abra un archivo PDF especialmente diseñado y ejecute código arbitrario en el sistema.</p> <p>La vulnerabilidad de severidad alta, identificada por MITRE como CVE-2024-0333 de tipo error de validación de entrada, existe debido a una validación de entrada incorrecta al procesar contenido HTML en Extensiones de Google Chrome. Un atacante remoto puede engañar a la víctima para que abra una página web especialmente diseñada y ejecute código arbitrario en el sistema de destino.</p> <p>La vulnerabilidad de severidad media, identificada por MITRE como CVE-2024-21337 de tipo permisos, privilegios y controles de acceso, existe debido a restricciones de seguridad impuestas incorrectamente. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado con el navegador y comprometer el sistema afectado.</p> <p>La vulnerabilidad de severidad media, identificada por MITRE como CVE-2024-20675 de tipo omisión de funciones de seguridad, existe debido a un error no especificado en Microsoft Edge. Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado y engañarla para que descargue o actualice una extensión potencialmente peligrosa.</p> <p>Se han asignado los siguientes identificadores para las vulnerabilidades de severidad baja: CVE-2024-48631 y CVE-2024-20721.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Microsoft Edge: 79.0.309.71 - 120.0.2210.121. <p>3. RECOMENDACIÓN:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades. 				
Fuente de Información:	<ul style="list-style-type: none"> • hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-20709 • hxxp://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21337 • hxxp://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20675 • hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-20721 • hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-48631 • hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-0333 			