

	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°050</b>		<b>Fecha: 27-02-2024</b>
Componente que reporta	<b>CENTRO NACIONAL DE SEGURIDAD DIGITAL</b>		
Nombre de la alerta	Vulnerabilidad crítica en la plataforma Azure de Microsoft		
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>Nitesh Surana (@_niteshsurana) de Trend Micro Research, ha reportado una vulnerabilidad de severidad <b>CRÍTICA</b> de tipo elemento de ruta de búsqueda no controlado en Azure de Microsoft. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario.</p> <p><b>2. DETALLES:</b></p> <p>Azure es la plataforma de servicios en la nube de Microsoft que ofrece una amplia gama de servicios para ayudar a las organizaciones a construir, implementar y administrar aplicaciones y servicios a través de Internet.</p> <p>La vulnerabilidad de severidad <b>crítica</b>, de tipo elemento de ruta de búsqueda no controlado, señala que cuando se instala desde Microsoft Container Registry, la instalación intenta cargar un recurso de nube inexistente que es vulnerable a la adquisición. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en sistemas que dependen del recurso de la nube.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>– MCR VSTS CLI para Microsoft Azure.</li> </ul> <p><b>3. RECOMENDACIÓN:</b></p> <ul style="list-style-type: none"> <li>• Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.</li> </ul>			
Fuente de Información:	<ul style="list-style-type: none"> <li>• <a href="https://www.zerodayinitiative.com/advisories/ZDI-24-208/">https://www.zerodayinitiative.com/advisories/ZDI-24-208/</a></li> </ul>		