

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°288			Fecha: 03-12-72023
				Página: 4 de 7
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL			
Nombre de la alerta	Ataques Activos Dirigidos A Google Chrome Y Defectos De OwnCloud			
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>La CISA anunció dos ataques activos de vulnerabilidades explotadas conocidas dirigidas a Google Chrome y vulnerabilidades de la propia nube en su catálogo.</p> <p>2. DETALLES:</p> <p>CVE-2023-6345:</p> <p>Un atacante remoto que se hubiera infiltrado en el proceso de renderizado podría haber podido realizar un escape del sandbox utilizando un archivo malicioso gracias a un desbordamiento de enteros en Skia en versiones de Google Chrome anteriores a 119.0.6045.199.</p> <p>El rango de gravedad de esta vulnerabilidad es Alto. La vulnerabilidad se encuentra actualmente en proceso de investigación.</p> <p>CVE-2023-49103:</p> <p>Esto se basa en una biblioteca GetPhpInfo.php de terceros que proporciona una URL y revela la información de configuración del entorno PHP. La información contiene los datos más confidenciales, como la contraseña de administrador de ownCloud, las credenciales del servidor de correo y la clave de licencia.</p> <p>Además, phpinfo pone a disposición muchos otros detalles de configuración potencialmente confidenciales que un atacante podría utilizar para aprender más sobre el sistema. Por lo tanto, esta vulnerabilidad debería seguir siendo motivo de preocupación incluso si ownCloud no opera en un contexto contenedorizado.</p> <p>El rango de gravedad de esta vulnerabilidad es crítico (10,0) y también se encuentra bajo proceso de inversión.</p>				
				
<p>3. RECOMENDACIÓN:</p> <ul style="list-style-type: none"> • Actualizar los paquetes afectados con las últimas versiones de software disponible que los proveedores lancen para abordar estas vulnerabilidades. 				
Fuente de Información:	<ul style="list-style-type: none"> • https://gbhackers.com/cisa-warns-google-chromeflaws/ 			