

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°283			Fecha: 27-11-2023
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA			
Nombre de la alerta	Vulnerabilidades en el complemento UserPro para WordPress			
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 dos vulnerabilidades de severidad MEDIA de tipo autorización inadecuada y permisos, privilegios y controles de acceso en el complemento UserPro para WordPress. La explotación exitosa de estas vulnerabilidades permite a un atacante remoto eludir las comprobaciones de autorización y a un usuario remoto escalar privilegios en el sistema.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad media, identificada por MITRE como CVE-2023-6007 de tipo autorización inadecuada, existe debido a que falta una verificación de capacidad en múltiples funciones. Un atacante remoto puede agregar, modificar o eliminar opciones de meta y complementos del usuario. Esta vulnerabilidad, no realiza o realiza incorrectamente una verificación de autorización cuando un actor intenta acceder a un recurso o realizar una acción.</p> <p>La vulnerabilidad de severidad media, identificada por MITRE como CVE-2023-6009 de tipo permisos, privilegios y controles de acceso, existe debido a que la aplicación no impone adecuadamente restricciones de seguridad en la función "userpro_update_user_profile", lo que conduce a la elusión de restricciones de seguridad y a una escalada de privilegios.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> - UserPro - Community and User Profile WordPress Plugin: 4.9.2 - 5.1.1. - UserPro - Community and User Profile WordPress Plugin: 4.9.2 - 5.1.4. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la última versión de software disponible para abordar estas vulnerabilidades. 				
Fuente de Información:	<ul style="list-style-type: none"> • https://www.wordfence.com/threat-intel/vulnerabilities/id/6c4f8798-c0f9-4d05-808e-375864a0ad95?source=cve • https://codecanyon.net/item/userpro-user-profiles-with-social-login/5958681 • https://www.wordfence.com/threat-intel/vulnerabilities/id/e8bed9c0-dae3-405e-a946-5f28a3c30851?source=cve • https://packetstormsecurity.com/files/175871/WordPress-UserPro-5.1.x-Password-Reset-Authentication-Bypass-Escalation.html 			