CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: 15/09/2023

Problemática: Alerta por Seguridad de módulos en Wordpress

Correlativo: AC-0070

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Sitios web desarrollados con el administrador de contenidos CMS WordPress fueron contaminados por malware que afectó diversos temas (templates) y plugins.

SITUACIÓN

Funciones programadas por terceros y agregadas al CMS de Wordpresss alojaron y permitieron la distribución del malware WP-VCD, cepa de infección dirigida al administrador de contenidos, este tipo de amenazas son conocidas por su uso de temas pirateados para su distribución.

La vulnerabilidad requiere de un usuario autenticado lo que hace mucho más difícil de explotar para un atacante, especialmente si requiere privilegios de nivel de administrador.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alta**

RECOMENDACIONES

Ante esta problemática, se recomienda siempre verificar la fuente de módulos como temas y plugins que puedan afectar de una forma crítica el contenido de los sitios, así se podrá limitar la distribución de malware.

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.

REFERENCIAS

WORDPRESS
https://ithemes.com/blog/wordpress-vulnerabilities-explained/