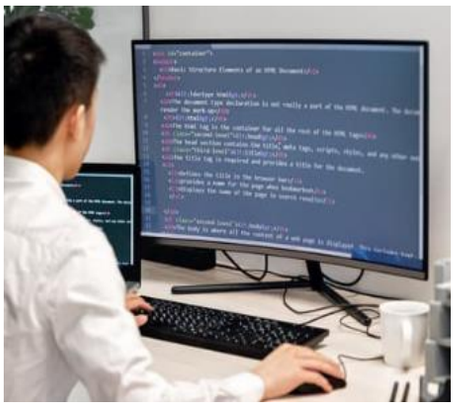
ALERTA

Vulnerabilidad Crítica en WPML (CVE-2024-6386)

COLCERT AL-2808-040

TLP:CLEAR

Se ha detectado una vulnerabilidad crítica (CVE-2024-6386) en el popular plugin de WordPress, WPML, que afecta a más de un millón de sitios web. Esta falla permite la ejecución remota de código (RCE) a través de una inyección de plantilla del lado del servidor (SSTI), lo que otorga a los atacantes control total sobre los sistemas comprometidos.



ELEMENTOS DE INTELIGENCIA DISPONIBLES

La vulnerabilidad radica en una sanitización inadecuada de la entrada del usuario en las plantillas Twig utilizadas por WPML. Un atacante podría inyectar código malicioso en estas plantillas, lo que permitiría ejecutar comandos arbitrarios en el servidor.

ANÁLISIS

La vulnerabilidad CVE-2024-6386 en WPML destaca la importancia de mantener los plugins y software actualizados. Los desarrolladores deben priorizar la seguridad en el diseño y desarrollo de software, y los usuarios deben ser proactivos en la aplicación de parches de seguridad. La rápida detección y respuesta a las vulnerabilidades son fundamentales para proteger los sistemas y datos de las organizaciones..

IMPACTO PARA COLOMBIA Y LA REGIÓN

Robo de datos: Los atacantes podrían acceder a bases de datos y robar información confidencial, como credenciales de usuarios, datos financieros y propiedad intelectual.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://securityaffairs.com/167673/hacking/wpml-wordpress-plugin-rce-1m-websites.html
https://thecyberexpress.com/wpml-plugin-flaw-wordpress-rce/
https://www.csa.gov.sg/alerts-advisories/security-bulletins/2024/sb-2024-035

COLCERT