BOLETÍN DE ALERTA

Boletín Nro.: 2017-01
Fecha de publicación: 27/01/2017
Tema: Vulnerabilidades críticas en Wordpress

Sistemas afectados:

- Wordpress desde la versión 4.7.1 y previas

Descripción:

Se ha reportado varias vulnerabilidades, dos de ellas críticas, que afectan a Wordpress, desde la versión 4.7.1 y previas.

Una de ellas es una vulnerabilidad de inyección SQL presente en la clase WP_Query, a través de la cual puede inyectarse datos no sanitizados. Si bien, dicha vulnerabilidad no afecta al core de Wordpress de forma directa, muchos plugins y temas podrían utilizar dicha clase, lo que introduciría la vulnerabilidad de SQLi en el sitio web afectado.

Una vulnerabilidad de Cross-Site Scripting (XSS) se encuentra en la porción de código que interactúa con la tabla de lista de posts.

Además, se encontró que el panel de administración del usuario, la sección de "Press This" en la que permite asignar términos de taxonomía es visible a usuarios que no tienen el permiso de utilizarlo.

Wordpress ha lanzado una actualización para dichas vulnerabilidades en la versión 4.7.2.

Impacto

Explotando algunas de estas vulnerabilidades un atacante remoto no autorizado podría obtener un control total del servidor que aloja la aplicación de Wordpress vulnerable.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Solución

Wordpress ha publicado una actualización, Wordpress 4.7.2 la cual corrige las vulnerabilidades. Se recomienda actualizar los sitios afectados de inmediato. La nueva versión puede ser obtenida aquí:

https://wordpress.org/download/

También se puede actualizar desde el panel de administración, ingresando a "Escritorio" > "Actualizaciones".

Puede leer la guía oficial de actualización de Wordpress aquí:

https://codex.wordpress.org/es:Actualizar_WordPress

Información adicional:

https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/

https://codex.wordpress.org/es:Actualizar_WordPress

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py