BOLETÍN DE ALERTA

Boletín Nro.: 2016-01
Fecha de publicación: 06/01/2016
Tema: Vulnerabilidad crítica de XSS en Wordpress

Sistemas afectados:

- Wordpress desde la versión 4.4 y previas

Descripción:

Se ha reportado una vulnerabilidad crítica de *Cross Site Scripting* (XSS) que afecta a Wordpress 4.4 y a las versiones previas. No han trascendido detalles acerca de la vulnerabilidad.

Wordpress ha publicado una nueva versión, 4.4.1, la cual corrige la vulnerabilidad. Además, la nueva versión corrige un total de 52 fallos funcionales (*bugs*), de los cuales uno de ellos se considera grave.

Entre los más destacado, se encuentran:

- Soporte de los últimos caracteres emoji
- Corrección de fallo que evitaba que sitios que utilizan versiones viejas de OpenSSL se comuniquen con otros servicios proveídos por ciertos plugins
- Problema de redirección cuando una URL de una publicación era reutilizada.

Para conocer la lista completa de cambios, puede leer:

https://core.trac.wordpress.org/query?milestone=4.4.1

Impacto

Un atacante remoto no autorizado podría obtener un control total del servidor que aloja una aplicación web construida con una versión vulnerable de Wordpress.

Solución

Wordpress ha publicado una actualización, Wordpress 4.4.1 la cual corrige la vulnerabilidad. Se recomienda actualizar los sitios afectados de inmediato. La nueva versión puede ser obtenida aquí:

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

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/2016/01/wordpress-4-4-1-security-and-maintenance-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