BOLETÍN DE ALERTA

Boletín Nro.: 2016-08
Fecha de publicación: 09/05/2016
Tema: Vulnerabilidades críticas en Wordpress

Sistemas afectados:

- Wordpress desde la versión 4.5.1 y previas

Descripción:

Se ha reportado dos vulnerabilidades críticas que afectan a Wordpress. Una vulnerabilidad de *Same-Origin Method Execution* afecta a Plupload, la librería utilizada en Wordpress, afectando así a todas las versiones previas a 4.5.2. Se trata de una técnica de ataque que abusa de las llamadas de retorno, principalmente los applets de Flash y JSONP a la que los cuadros de diálogo de OAuth normalmente redireccionan (redirect_uri), forzando a la víctima a la ejecución de métodos arbitrarios de cualquier página en el dominio del punto final. Esta técnica es utilizada para evadir Políticas de Mismo Origen (*Same-Origin Policies* - SOP).

Además, las versiones de WordPress desde 4.2 a 4.5.1 son vulnerables a XSS reflejado utilizando URI especialmente diseñados a través MediaElement.js, la biblioteca de terceros utilizado para reproductores de medios.

Wordpress ha lanzado una actualización para dichas vulnerabilidades en la versión 4.5.2. MediaElement.js y Plupload también han publicado actualizaciones que corrigen estos problemas.

Impacto

El impacto y la criticidad dependerán de la aplicación. En algunos casos, un atacante remoto no autorizado podría obtener un control total de la sesión de usuario que explota, pudiendo obtener acceso a información sensible de forma no autorizada. En caso de tratarse de una sesión de usuario con privilegio de administrador, podría obtener el 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 4.5.2 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/2016/05/wordpress-4-5-2/

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

http://www.benhayak.com/2015/06/same-origin-method-execution-some.html

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