Vulnerabilidad En Plugin De WordPress Que Afecta Millones De Descargas

Vulnerabilidad En Plugin De WordPress Que Afecta Millones De Descargas

Una nueva vulnerabilidad se ha descubierto en el **plugin WPTouch de WordPress**, el cual pone al descubierto una serie de fallas que afectan críticamente algunos plugins activos descargados y utilizados por millones de bloggers que usan el CMS WordPress.

Desde mayo, la compañía de seguridad Sucuri ha encontrado graves agujeros de seguridad en el plugin WPTouch con (5.670.626 descargas), Disqus (1.400.003 descargas), All In One SEO Pack (19,152,355 descargas), y MailPoet Newsletters (1,894,474 descargas). Si es un usuario de WordPress y estás usando en este momento cualquiera de estos plugins, es mejor que corras a actualizar de inmediato estos plugins.

Todos los fallos de seguridad han sido parcheado en las nuevas versiones de cada plugin. Las diversas vulnerabilidades pueden permitir a un atacante utilizar su sitio web con señuelo para el phishing, enviar SPAM, usarte como un host de malware sin saberlo, infectar otros sitios (si estas en un servidor compartido), y mucho mas.

En el administrador de plugins, compruebe que dispone de las siguientes versiones actuales de cada plugin afectado:

- WPTouch (3.4.3)

- Disqus (2.77)
- All In One SEO Pack (2.2.1)
- MailPoet Newsletters (2.6.9)

El más reciente hallazgo de **Sucuri**, es la vulnerabilidad en el plugin para dispositivos móviles, WPTouch, permitiendo a los atacantes subir archivos PHP maliciosos o backdoors al servidor de destino sin necesidad de privilegios de administrador.

El agujero de seguridad ha sido descubierto el lunes por **Sucuri**, que en realidad es un **error en el código de WPTouch,** permitiría a un atacante apropiarse con tu sitio web, y lo peor, no habrá manera de que sepas que estas hackeado.

El lunes, inmediatamente se descubrio el fallo, la compañía anuncio en su blog la falla:

> *Durante una auditoría de rutina para nuestra WAF, descubrimos una vulnerabilidad muy peligrosa que podría permitir a un usuario sin privilegios administrativos, que se conecta (como un suscriptor o un autor), subir archivos de PHP en el servidor de destino.*
>
> *Alguien con malas intenciones podría subir backdoors PHP u otro malware malicioso y, básicamente, tomar el control del sitio web. Así que para hacer no hacer un cuento largo, si está ejecutando WPtouch, a continuación, actualice de inmediato!*

Las datos especificados de los investigadores: «Este descubrimiento sólo se aplica a las versiones 3.x de WPtouch. Aquellos sitios que usen versiones 2.x y 1.x del plugin no se verán afectados por la vulnerabilidad.»

Sucuri también señaló que «esta vulnerabilidad sólo puede usarse si su sitio web permite a los usuarios invitados registrarse.»

La noticia llega tras una serie de descubrimientos recientes que revelan un considerable número de exploits y vulnerabilidades de grave preocupación para cualquier persona que ejecute una instalación de WordPress.

Actualizar Los Plugins Ó ….

El 1 de julio el equipo de seguridad encontró un grave vulnerabilidad en el plugin MailPoet, en el cual anunciaron: «Si tiene activado este plugin en su sitio web, las probabilidades no están a su favor. Un atacante puede explotar esta vulnerabilidad sin tener privilegios en las cuentas para apropiarse del sitio».

Este error debe ser tomado en serio, le da a un potencial intruso el poder para hacer lo que quiera en la página web de su víctima. Se permite cualquier archivo PHP pueda ser cargado.
Sucuri está en racha, ya que el 31 de mayo se encontraron dos vulnerabilidades graves en «All in One SEO Pack», un plugin ampliamente utilizado.

Por si alguien piensa que la vulnerabilidad en un plugin de SEO no es problema, escribieron:

> *Si bien, esto no se ve tan mal al principio, descubrimos que este error puede ser usado con otra vulnerabilidad para ejecutar código JavaScript malicioso en una panel de control del administrador.*
>
> *Ahora bien, esto significa que un atacante podría potencialmente inyectar cualquier código javascript y hacer*

> *cosas como cambiar la contraseña de cuenta del administrador para dejar alguna puerta trasera en los archivos de su sitio web con el fin de llevar a cabo incluso las actividades maliciosas, más adelante.*

Poco después del descubrimiento de las vulnerabilidades en SEO Pack, a finales de junio, los investigadores también descubrieron una falla de ejecución remota de código crítico (RCE) en el plugin popular de sistema de comentarios Disqus.

La cuestión Disqus sólo afecta a usuarios específicos de WordPress. Si bien la propia falla es bastante peligrosa, sólo puede ser activado en los servidores que utilizan WordPress con la versión de PHP 5.1.6 ó versiones anteriores.

Esto también significa que sólo los usuarios de WordPress 3.1.4 (o anterior) son vulnerables a ella, ya que las versiones más recientes no soportan estas versiones anteriores de PHP. WordPress es una plataforma de blogs bastante popular, esta presente en la gestión del contenido de algunos de los sitios web más leídos, y todo esto hace que WordPress sea un blanco perfecto para ser atacado.