Ungepatchte Schwachstelle im WordPress-Core: Was es wirklich bedeutet

Geschrieben von iThemes-Redaktionsteam an 14. Dezember 2022

Zuletzt aktualisiert am 14. Dezember 2022

Diese Woche Im iThemes Vulnerability Report werden Sie feststellen, dass es eine ungepatchte Schwachstelle im WordPress-Core gibt. Diese Schwachstelle wurde von Thomas Chauchefoin gemeldet und betrifft derzeit alle Versionen von WordPress. Die wahrscheinliche Ausnutzung dieser Schwachstelle ist jedoch sehr gering, und um sich vollständig zu schützen, müssen Sie lediglich XML-RPC oder Pingbacks auf Ihrer WordPress-Site deaktivieren.

Was diese Schwachstelle für Ihre Website bedeutet

Obwohl ein vollständiger Proof of Concept noch nicht von WPScan veröffentlicht wurde, können wir einige fundierte Vermutungen darüber anstellen, wie diese Schwachstelle ausgenutzt werden kann. Sie sagen:

> *„WordPress ist von einer nicht authentifizierten blinden SSRF in der Pingback-Funktion betroffen. Aufgrund einer TOCTOU-Rennbedingung zwischen den Validierungsprüfungen und der HTTP-Anfrage können Angreifer interne Hosts erreichen, die ausdrücklich verboten sind.“*

Um diese Schwachstelle auszunutzen, würde ein Angreifer WordPress-Pingbacks verwenden, wäre aber dazu gezwungen, dies in Kombination mit anderen Schwachstellen zu tun.

Um eine Schwachstelle wie diese auszunutzen, um einer WordPress-Site irgendeinen Schaden zuzufügen, wäre diese Schwachstelle nur nützlich, wenn sie mit anderen ernsteren Schwachstellen auf einer nicht gepatchten oder unsicheren WordPress-Site verwendet wird.

Offiziell hat das Sicherheitsteam von WordPress.org erklärt, dass es sich um eine Schwachstelle mit niedriger Priorität handelt. Insbesondere sagten sie dem Daily Swig :

> *„… dies ist ein Problem mit geringen Auswirkungen, und um es auszunutzen, muss es mit zusätzlichen Schwachstellen in Software von Drittanbietern [verkettet] werden. Daher betrachtet das Sicherheitsteam das Problem als gering.“*

Sie fügten hinzu: „Aufgrund seines geringen Schweregrades diskutiert das Team, ob dieses Problem als allgemeine Härtungsmaßnahme öffentlich behoben werden könnte.“

Dies unterstreicht die Schwierigkeit, Sicherheitsfixes zu so vielen älteren Versionen von WordPress hinzuzufügen. Jahrelang hat das Kernteam Patches auf Versionen zurückportiert, die viele Jahre alt waren und nur von wenigen Nachzüglerseiten verwendet wurden, die noch nicht aktualisiert wurden. Die jüngste Entscheidung des Kernteams, ältere Versionen nicht mehr zurückzuportieren, wird die Behebung dieser Art von Problemen für das WordPress-Kernteam einfacher und schneller machen.

So schützen Sie Ihre Website

Da Pingbacks der offensichtliche Schwachpunkt sind, der diskutiert wird, ist das Deaktivieren von Pingbacks und/oder XML-RPC ein guter erster Schritt.

Wenn Sie Ihre WordPress-Site auf dem neuesten Stand halten und sich auf einem zuverlässigen Hosting mit einer starken und sicheren Infrastruktur befinden, ist die Wahrscheinlichkeit

einer Ausnutzung dieser Schwachstelle extrem gering.

Wenn Sie Ihre Website so sicher wie möglich halten möchten, ist es am besten, Pingbacks oder XML-RPC zu deaktivieren. Glücklicherweise bietet Ihnen iThemes Security die Möglichkeit, beides zu tun.

So deaktivieren Sie XML-RPC mit iThemes Security

Das Deaktivieren von XML-RPC mit iThemes Security ist unglaublich einfach. Gehen Sie zu **Sicherheit > Einstellungen > Erweitert > WordPress-Optimierungen** und verwenden Sie dann das Dropdown-Menü, um XML-RPC zu deaktivieren.

Es kann Fälle geben, in denen Sie XML-RPC benötigen. Diese beinhalten:

- Wenn Sie eine alte Website haben, die Sie nicht auf Version 4.4 oder höher aktualisieren können, haben Sie keinen Zugriff auf die REST-API und verwenden möglicherweise Dienste, die XML-RPC erfordern.
- Sie verwenden ein Programm, das nicht auf die REST-API zugreifen kann, um mit Ihrer Website zu kommunizieren.
- Integration mit einigen Apps von Drittanbietern, die nur XML-RPC verwenden können.

Das Deaktivieren von XML-RPC ist mit iThemes Security ein einfacher Vorgang. Sie können dies ausschalten und die Funktionalität Ihrer Website testen, und wenn etwas nicht richtig zu funktionieren scheint, können Sie es wieder einschalten.

Dies sind Situationen, in denen es sinnvoll ist, einen Staging-Server einzurichten, damit Sie Änderungen testen können, bevor Sie sie auf Ihre Produktionssite anwenden.

Stummschalten der Schwachstelle in Ihrem iThemes Site Scan

Natürlich benachrichtigt Sie der Site-Scanner von iThemes Security über diese Schwachstelle. Da es in naher Zukunft nicht vom Kernteam behoben wird, könnte es sinnvoll sein, der Warnungsermüdung vorzubeugen, indem diese Schwachstelle im Site-Scanner stummgeschaltet wird. Weitere Informationen zum Stummschalten von Schwachstellenwarnungen finden Sie in unserer Hilfedokumentation .

Fazit

Obwohl diese Sicherheitsanfälligkeit nicht gepatcht ist, stellt sie ein sehr geringes Risiko für Besitzer von WordPress-Sites dar. Wenn auf Ihrer Website XML-RPC bereits deaktiviert ist, sind Sie bereits geschützt. Pingbacks sind eine der Legacy-Funktionen von WordPress, die in einigen Fällen nützlich sein können, aber es ist keine Funktion, die von vielen modernen Websites verwendet wird. Dies ist einer der Fälle, in denen es hilfreich ist, ein Sicherheits-Plugin wie iThemes Security installiert zu haben, damit Sie schnell Maßnahmen ergreifen können, um Ihre Website gegen Angreifer zu schützen, selbst wenn die betreffende Schwachstelle von geringer Schwere ist.