شبکه گستر

WordPress Cross-Site Scripting

آسیب‌پذیری WordPress در برابر حملات " تزریق کُد"

تهیه کننده: گروه تحقیق، توسعه و آموزش شرکت مهندسی شبکه گستر

تاریخ انتشار: اردیبهشت ۱۳۹۴

شماره: ۹۴-۰۲

معرفی

۵ اردیبهشت ۱۳۹۴، جزییات یک ضعف امنیتی از نوع تزریق کد (Cross-Site Scripting) در سامانه مدیریت محتوا WordPress به صورت عمومی منتشر شد.

نفوذگر با سواستفاده از این ضعف امنیتی و با تزریق کد JavaScript مخرب در فرم‌های "نقطه نظرات" (Comment Form) که در میلیون‌ها وبلاگ مورد استفاده قرار گرفته، می‌تواند در هنگام نمایش آن توسط مدیر سیستم (Administrator)، کد مخرب را به اجرا در آورد. بدین ترتیب نفوذگر قادر به تغییر دادن گذرواژه مدیر سیستم، ایجاد کاربر جدید و بطور کلی اجرا کردن تمام فرامینی است که مدیر سیستم دسترسی به آنها دارد.

دو روز پس از انتشار این خبر، موسسه WordPress، این ضعف امنیتی را با ارائه نگارش 4.2.1 ترمیم کرد.

در فاصله‌ای کوتاه، ضعف امنیتی دیگری در Genericons که بسته‌ای از نماد-قلم‌ها (Icon Font) است گزارش شد. یک فایل غیرامن بنام example.html در این بسته سبب ایجاد آسیب‌پذیری به حملات تزریق کد می شود و سواستفاده از آن در نتیجه ویرایش Document Object Model یا DOM در مرورگر امکان پذیر می‌گردد. تنظیمات DOM در مرورگر، نحوه دسترسی و نمایش فایلهای HTML و XML را مشخص می کند.

پوسته‌ها (Themes) و افزایه‌های (Plug-ins) بسیاری از Genericons استفاده می‌کنند.

این ضعف امنیتی نیز در نگارش 4.2.2 که روز پنج شنبه ۱۷ اردیبهشت عرضه شد، ترمیم شده است.

هر دو ضعف امنیتی در نگارش 4.2.2 که در تاریخ ۷ اردیبهشت ۹۴ ارائه شد ترمیم شده است.

WordPress معروف‌ترین سامانه مدیریت محتوای وبلاگ‌ها بر روی اینترنت است.

بهره‌جو (Exploit)

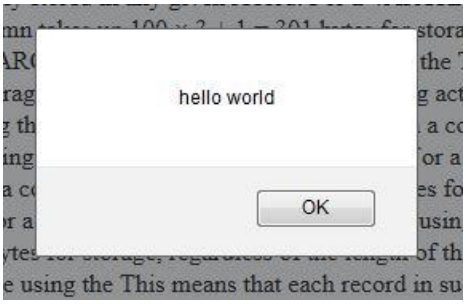
سواستفاده از Comment Form

فیلدهای از نوع TEXT در بانک داده‌های MySQL دارای محدودیت ۶۴ کیلوبایتی می‌باشند. بنابراین اگر داده‌های وارد شده در یک فیلد در بانک داده‌ها با نوع TEXT ذخیره شود و کاربر داده‌هایی بیش از ۶۴ کیلوبایت در آن فیلد وارد کرده باشد، MySQL داده‌ها را به تکه‌های ۶۴ کیلوبایتی تقسیم می‌کند. با این توصیف، در نسخه‌های آسیب‌پذیر، نفوذگر می‌تواند با وارد کردن عباراتی بسیار طولانی (بیش از ۶۴ کیلوبایت) و با جا سازی کدهای مخرب در آنها، در هنگام مشاهده داده‌ها توسط مدیر سیستم باعث اجرا شدن آن کدها شود.

برای نمونه در کدی که توسط کارشناس کاشف این ضعف ارائه شده است (شکل ۱)، هنگامی که مدیر سیستم نشانگر موشواره را بر روی فیلد قرار می‌دهد، پیامی با عنوان hello word ظاهر می‌شود (شکل ۲).

```
<a    title='x'    onmouseover='alert(unescape(/hello%20world/.source))'
style=position:absolute;left:0;top:0;width:5000px;height:5000px
AAAAAAAAAAAA...[64 kb]..AAA'></a>
```

▲ **شکل ۱:** کد نمونه ارائه شده توسط کاشف ضعف امنیتی (با اندکی تغییر)



▲ **شکل ۲: پنجره ظاهر شده در نتیجه اجرا شدن کد**

نمونه‌هایی از بهره‌جویی از این ضعف امنیتی گزارش شده است.

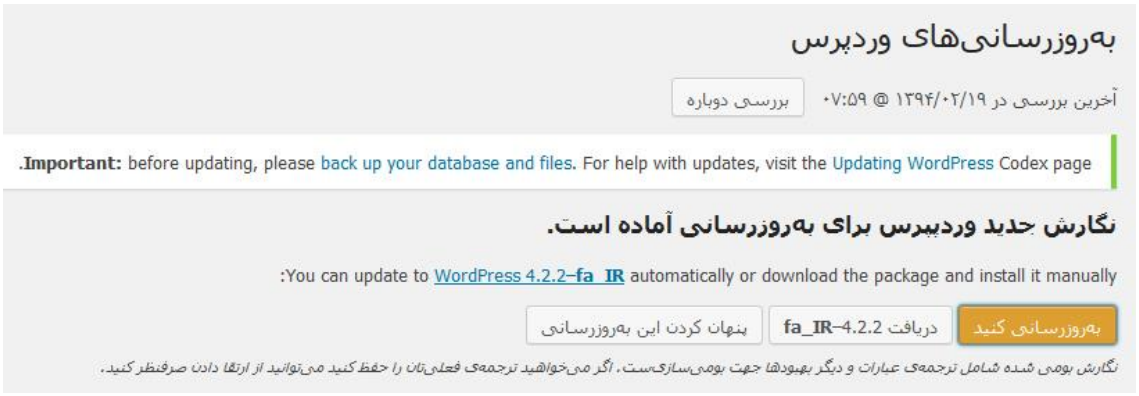
سوءاستفاده از Genericons

برای سوءاستفاده موفقیت‌آمیز از این ضعف امنیتی قربانی می‌بایست بر روی یک لینک مخرب کلیک کند. بر همین اساس، نفوذگر می‌تواند پس از شناسایی یک وب‌گاه آسیب‌پذیر، اقدام به ارسال ایمیلی حاوی پیوندی مخرب به کاربران آن وب‌گاه کند. با کلیک کاربر روی پیوندی حاوی بهره‌جو کوکی‌های (Cookies) کاربر تحت کنترل نفوذگر در خواهند آمد.

پس از نفوذ و دسترسی غیرمجاز، برنامه مخرب مستقیماً در مرورگر و بدون ارسال شدن به سرور اجرا می‌شود و در نتیجه حتی در صورت مجهز بودن سایت به دیواره آتش (Web Application Firewall) فرامین مخرب قابل اجرا خواهد بود.

پیشگیری

به مدیران وب‌گاه‌های مبتنی بر WordPress توصیه می‌شود در اسرع وقت، با مراجعه به صفحه پیشخوان، بخش به‌روزرسانی‌ها در WordPress اقدام به ارتقا به نگارش 4.2.2 کنند (شکل ۳).



▲ **شکل ۳: بخش به‌روزرسانی WordPress**

نگارش 4.2.2 از اینجا نیز قابل دریافت می‌باشد.

پیوندهای مفید

- WordPress 4.2 Stored XSS:
  http://klikki.fi/adv/wordpress2.html

- DOM XSS Vulnerability in Twenty Fifteen WordPress Theme:
  https://www.netsparker.com/cve-2015-3429-dom-xss-vulnerability-in-twenty-fifteen-wordpress-theme/

- DOM Based Cross-site Scripting Vulnerability:
  https://www.netsparker.com/blog/web-security/dom-based-cross-site-scripting-vulnerability/

- US-CERT: WordPress Releases Security Update
  https://www.us-cert.gov/ncas/current-activity/2015/04/27/WordPress-Releases-Security-Update

- US-CERT: WordPress Security and Maintenance Release
  https://www.us-cert.gov/ncas/current-activity/2015/05/07/WordPress-Security-and-Maintenance-Release

شبکه گستر

شرکت مهندسی شبکه گستر

گروه فروش ۵۷ – ۸۸ ۶۵ ۸۲ ۵۳ | sales@shabakeh.net

گروه پشتیبانی ۸۵ – ۸۸ ۲۰ ۲۴ ۸۱ | support@shabakeh.net

تارنمای شرکت www.shabakeh.net

سامانه پشتیبانی help.shabakeh.net

پایگاه اطلاع رسانی blog.shabakeh.net

خدمات پس از فروش my.shabakeh.net