

# آسیب پذیری یکی از افزونه‌های وردپرس وبسایت را در اختیار مهاجمین قرار می‌دهد - دیجیاتو

مانی میرجوادی | جمعه، ۲۶ بهمن ۱۳۹۷

اگر صاحب وب سایت هستید و از نرم افزار مدیریت محتوای وردپرس استفاده می‌کنید باید مراقب باشید که یک افزونه‌ی جدید وردپرس به نام [Simple Social Buttons](#) می‌تواند کل وبسایتتان را در اختیار مهاجمین قرار دهد.

افزونه‌ی یاد شده عموماً به منظور اشتراک گذاری فایل‌های صوتی و تصویری در فضای مجازی مورد استفاده قرار می‌گیرد.

«لوکا سیکیچ» توسعه دهنده و محقق امنیت وردپرس از شرکت WebARX هفته‌ی گذشته یک آسیب پذیری در Simple Social Buttons پیدا کرد و آن را به اطلاع سازنده‌ی پلاگین گزارش داد.

در [گزارش منتشر شده](#) از سوی سیکیچ که روز گذشته منتشر شد، او معضل یاد شده را به خاطر ایراد در طراحی اپلیکیشن و عدم استفاده از زنجیره‌ی مناسب برای تایید رمز عبور دانسته است. او بر این عقیده است که مهاجم می‌تواند با ثبت نام حساب‌های کاربری جدید در سایت از آسیب پذیری موجود استفاده کرده و به آن نفوذ کند.



سیکیچ همچنین با انتشار یک ویدیو نشان داد که چگونه می‌توان با استفاده از این آسیب پذیری به کلیدی ترین اطلاعات وبسایت نفوذ پیدا کرد. او این کار را در ویدیو با تغییر ایمیل ادمین سایت انجام داده می‌دهد. (ویدیو در انتهای مطلب)

بعد از ارائه‌ی گزارش سیکیچ به وبسایت شرکت سازنده‌ی این پلاگین یعنی WPBrigade، نسخه‌ی 2.0.22 عرضه شد که توصیه می‌شود کاربران از این نسخه استفاده کنند.

البته وجود این آسیب پذیری در پلاگین همیشه باعث از دست رفتن سایت نمی‌شود. برخی از ادمین‌ها به صورت پیش فرض امکان ایجاد حساب کاربری را به خاطر مسائل امنیتی از وبسایت سلب کرده‌اند. به همین دلیل این پلاگین حتی با وجود آسیب پذیری تهدیدی برای سایت محسوب نخواهد شد.

اما وب سایت‌هایی که به کاربران اجازه می‌دهند تا با عضو شدن در وبسایت زیر پست‌های خبری نظر درج کنند، در صورت استفاده از این افزونه در معرض خطر قرار خواهند گرفت.

این پلاگین در بیش از ۴۰ هزار وبسایت در سرتاسر دنیا مورد استفاده قرار می‌گیرد و در حال حاضر وجود این آسیب پذیری می‌تواند موقعیتی مناسب برای مهاجمین و خرابکاران سایبری برای به دست گرفتن وبسایت‌ها باشد.

در ادامه می‌توانید ویدیوی منتشر شده توسط سیکیچ را مشاهده کنید:

[دیجیاتو](#)