
***Issued 2/14/17***

## Over A Million WordPress Sites Defaced

The WordPress saga is nowhere near over as people still lag behind on updating to the latest version. Now, the number of defaced websites has passed the million mark. The speed with which this situation is escalating is a good reason to worry, but there's not much to be done if people don't update to the latest WordPress version, as they were advised to do weeks ago.

If you'll remember, back on January 26, WordPress released a new security fix, just weeks after its latest update. The new version contained a security fix for a vulnerability allowing attackers to modify content on a WordPress site. The company simply made the announcement about the three features they were fixing and was done with it, going into silent mode for a week. Then, seven days later, WordPress came back and expressed why it had made the security update and why it provided no explanation for it. The secret feature they were actually, really fixing had not been previously divulged, and it was clear from the announcement that it had been a calculated decision.

WordPress was hoping that people would make the update in the week that passed, thus protecting their websites. By the time the announcement came, a substantial number of WordPress sites had made the update, especially since many of them had the feature automated. One week later it was announced that about 100,000 websites had been defaced. Another

week has passed, and the situation has gone from bad to worse. WordFence, a team of software engineers providing plugins for WordPress, reports an uptick in REST- API exploits, with the number rising to over a million. “Attacks continued and February 6th we saw attackers had discovered a new variant on the attack which bypassed our rule and the rules that other firewall vendors had put into place,” explains CEO Mark Maunder in a blog post. “This vulnerability has resulted in a kind of feeding frenzy where attackers are competing with each other to deface vulnerable WordPress websites. During the past 48 hours, we have seen over 800,000 attacks exploiting this specific vulnerability across the WordPress sites we monitor.” This vulnerability has resulted in a kind of feeding frenzy where attackers are competing with each other to deface vulnerable WordPress websites.

During the past 48 hours we have seen over 800,000 attacks exploiting this specific vulnerability across the WordPress sites we monitor,” he adds. They said they are now tracking 20 separate defacement campaigns, a great hike from the three we saw within the first few days. One of them, MuhmadEmad is responsible for over 350,000 of these defacements. Sucuri’s experts warn that attackers are trying to exploit sites that have plugins like the Insert PHP, Exec-PHP and others similar to these. The vulnerability allows attackers to execute PHP code when injecting their content into the database.