Researchers find serious flaws in WordPress plugins used on 400k sites



reader comments

49 with 33 posters participating

Share this story

Serious vulnerabilities have recently come to light in three WordPress plugins that have been installed on a combined 400,000 websites, researchers said. InfiniteWP, WP Time Capsule, and WP Database Reset are all affected.

The highest-impact flaw is an authentication bypass vulnerability in the InfiniteWP Client, a plugin installed on more than 300,000 websites. It allows administrators to manage multiple websites from a single server. The flaw lets anyone log in to an administrative account with no credentials at all. From there, attackers can delete contents, add new accounts, and carry out a wide range of other malicious tasks.

People exploiting the vulnerability need only know the user name of a valid account and include a malicious payload in a POST request that's sent to a vulnerable site. According to Web application firewall provider Wordfence, the vulnerability stems from a feature that allows legitimate users to automatically log in as an administrator without providing a password.

"Logical vulnerabilities like the ones seen in this recent disclosure can result in severe issues for Web applications and components," Marc-Alexandre Montpas, a researcher at Web

security firm Sucuri, wrote in a post. “These flaws can be exploited to bypass authentication controls—and in this case, log in to an administrator account without a password.”

Anyone running InfiniteWP Client version 1.9.4.4 or earlier should update to 1.9.4.5 immediately.

The critical flaw in WP Time Capsule also leads to an authentication bypass that allows unauthenticated attackers to log in as an administrator. WP Time Capsule, which runs on about 20,000 sites, is designed to make backing up website data easier. By including a string in a POST request, attackers can obtain a list of all administrative accounts and automatically log in to the first one. The bug has been fixed in version 1.21.16. Sites running earlier versions should update right away. Web security firm WebARX has more details.

The last vulnerable plugin is WP Database Reset, which is installed on about 80,000 sites. One flaw allows any unauthenticated person to reset any table in the database to its original WordPress state. The bug is caused by reset functions that aren’t secured by the standard capability checks or security nonces. Exploits can result in the complete loss of data or a site reset to the default WordPress settings.

A second security flaw in WP Database Reset causes a privilege-escalation vulnerability that allows any authenticated user—even those with minimal system rights—to gain administrative rights and lock out all other users. All site administrators using this plugin should update to version 3.15, which patches both vulnerabilities. Wordfence has more details about both flaws here.

There’s no evidence that any of the three vulnerable plugins are being actively exploited in the wild.

https://arstechnica.com/?p=1645061