Plugin vulnerability finders tell WordPress users to update asap

January 21 2020, by Nancy Cohen

Credit: CC0 Public Domain

Three WordPress plugins have been picking up quite the glare of attention this month after researchers found serious vulnerabilities in them—and the numbers are sobering, in that these plugins have been installed on more than 400,000 websites—with users too wide open for cyberattacks to ignore.

The three plugins in the spotlight were InfiniteWP, WP Time Capsule, and WP Database Reset plugins.

ZDNet was one of the tech watching sites to prod readers to action: "If you use these plugins you should update immediately as firewall l protection will not work."

HotHardware's Brittany Goetting offered some more grim numbers. There are over 50,000 plugins to go round and not all are created equal, she wrote.

Out of the three in the spotlight, one may as well begin with the authentication bypass vulnerability in the InfiniteWP Client. *Naked Security* described it as a tool that allows admins to manage multiple WordPress sites from the same interface.

Administrators overseeing sites use InfiniteWP Client.

At least 300,000 of sites could have been affected by the vulnerability, Goetting said.

The plugin, it was found, lacked certain authorization checks. "You are vulnerable if you are using InfiniteWP Client versions up to 1.9.4.4, and as a result users of the plugin should update their sites to version 1.9.4.5 as soon as possible," she wrote.

The Wordfence blog (Wordfence is product of a company called Defiant) said this was a critical authentication vulnerability. "A proof of concept was published this morning, January 14, 2020. If you are using InfiniteWP client version 1.9.4.4 or earlier we recommend immediately updating your installation to protect your site."

Dan Goodin in *Ars Technica* also described the seriousness of the

authentication bypass vulnerability in InfiniteWP Client plugin.

"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."

Security company WebARX reported InfiniteWP Client, and another vulnerability, WP Time Capsule.

The WP Time Capsule was designed to make backing up website data easier.

Ars Technica reported that the bug had been fixed in version 1.21.16. "Sites running earlier versions should update right away. Web security firm WebARX has more details." said *Ars*.

ZDNet talked about WP Time Capsule; Charlie Osborne in *ZDNet* said that WP Time Capsule was active on at least 20,000 domains, according to the WordPress plugins library.

The WP Database Reset plugin received much attention, with nearly 80,000 sites using the plugin, which helps users to reset their databases or parts of databases to their default settings.

Wordfence: "On January 7th, our threat Intelligence team discovered vulnerabilities in WP Database Reset, a WordPress plugin installed on over 80,000 websites. One of these flaws allowed any unauthenticated user to reset any table from the database to the initial WordPress set-up state, while the other flaw allowed any authenticated user, even those with minimal permissions, the ability to grant their account administrative privileges while dropping all other users from the table with a simple request."

The plugin did not initially include the proper security checks. "One vulnerability allowed attackers to reset any table and cause a loss of data availability," wrote Goetting. "Another vulnerability enabled any subscriber to take full control of the website and kick out all administrators. Both flaws have thankfully been fixed with version 3.15. Of course the security researchers also encourage users to always back up their sites."

Sergiu Gartlan for *BleepingComputer* paid attention to that finding too. "Critical bugs found in the WordPress Database Reset plugin ...allow attackers to drop all users and get automatically elevated to an administrator role and to reset any table in the database."

The Wordfence blog issued this advice, seeing that these were considered critical security issues that could cause complete site reset and/or takeover. "We highly recommend updating to the latest version (3.15) immediately."

What did *Ars Technica* conclude about the three plugins, InfiniteWP, WP Time Capsule, and WP Database Reset? They had few words and these came easily: "It's time to patch."

Readers' comments in Ars were attempting to pinpoint the source of the problems. "The problem," said one reader, "is when site admins install 10,000 plugins, each of which becomes a new vector for attack."

Where did users hear that before? *Computer Business Review*, back in June, declared that "WordPress Plugins are widely regarded to be one of the single greatest security threats to WordPress users."

There's no evidence that any of the three vulnerable plugins are being actively exploited in the wild, said Goodin.

More information: blog.sucuri.net/2020/01/authen … finitewp-client.html

Citation: Plugin vulnerability finders tell WordPress users to update asap (2020, January 21) retrieved 27 April 2024 from https://techxplore.com/news/2020-01-plugin-vulnerability-finders-wordpress-users.html