WordPress plug-in for Zero-day exploited in the wild

17 hours ago

NEWS by Doug Olenick

Hackers are continuing to abuse the recently patched zero day vulnerability in the WordPress plugin Easy WP SMTP that if exploited can give attackers administrative control of a site.

Hackers are continuing to abuse the recently patched zero day vulnerability in the WordPress plugin Easy WP SMTP that if exploited can give attackers administrative control of a site.

The zero day was first exploited in the wild for version 1.3.9 on March 15 and WordPress issued an update to pushing out version 1.3.9.0 on March 17. The organization also released a firewall rule to prevent exploitation of the flaw for those with WordPress Premium who have not yet updated their system.

Free users will gain access to the firewall in 30 days, but can protect themselves immediately by downloading the latest version of the plugin.

The plugin, which is installed on 300,000 sites, allows users to configure SMTP connections for outgoing email.

"The root of the vulnerability is in the Import/Export functionality which was added to Easy WP SMTP in version 1.3.9.," the WordPress team reported.

Wordfence's Defiant Threat Intelligence team is now tracking to distinct groups using the zero day to launch attacks. In both cases the attack scheme is the same as the proof of concept put forth in NinTechNet's March 17 disclosure. Here the attackers exploit the flaw to create a new admin user account to gain control.

At this point the attackers take separate paths.

In one case no additional activity takes place, which Wordfence believes could mean this portion of the attack was automatic and the malicious actors are compiling a number of account for future use.

"The other campaign continues by altering the victim site's siteurl and home options to trigger malicious redirects when the site is visited, then injecting malicious <script> tags into all PHP files on the affected site with the string "index" present in their name. This obviously affects files named index.php, but also happens to impact files like class-link-reindex-post-service.php, present in Yoast's SEO plugin," Wordfence wrote.

In the latter scheme assigns tracking codes and cookies to track the newly compromised accounts and then use the information to redirect them to malicious sites, usually those supporting tech support scams or Zeus malware.

Brandon Chen, digital security and operations manager for The Media Trust , said plugins can be problematical for users.

"Each plugin represents at least a few attack surfaces, because the code that enables the plugin to function is coming from at least one vendor, who likely bringing in outsourced code. In short, every plugin you introduce into your digital environment introduces third parties you may or may not know—and chances are, you don't know most of them," he said.

This article was originally published on SC Media US.

Topics: SECURITY PATCHING SOFTWARE VULNERABILITIES