

Hackers actively exploit WordPress plugin flaw to send visitors to bad sites

Enlarge / A redirection from a site still running a vulnerable version of the plugin.

reader comments

24 with 21 posters participating

Share this story

Hackers have been actively exploiting a recently patched vulnerability in some websites that causes the sites to redirect to malicious sites or display misleading popups, security researchers warned on Wednesday.

The vulnerability was fixed two weeks ago in WP Live Chat Support, a plugin for the WordPress content management system that has 50,000 active installations. The persistent cross-site scripting vulnerability allows attackers to inject malicious JavaScript into sites that use the plugin, which provides an interface for visitors to have live chats with site representatives.

Researchers from security firm Zscaler's ThreatLabZ say attackers are exploiting the vulnerability to cause sites using unpatched versions of WP Live Chat Support to redirect to malicious sites or to display unwanted popups. While the attacks aren't widespread, there have been enough of them to raise concern.

"Cybercriminals actively look for new vulnerabilities in

popular content management systems such as WordPress and Drupal, as well as popular plugins that are found in many websites,” Zscaler’s Prakhar Shrotriya wrote in a post. “An unpatched vulnerability in either the CMS or associated plugins provides an entry point for attackers to compromise the website by injecting malicious code and impacting the unsuspecting users visiting these sites.”

The vulnerability lets anyone visiting the site update the plugin settings by calling an unprotected “admin_init hook” and injecting malicious JavaScript anywhere the Live Chat Support icon appears. The attacks observed by Zscaler use the injected script to send a request to `hxxps://blackawardago[.]com` to execute the main script. Visitors are then redirected to multiple URLs that push unwanted popup ads, fake error messages, and requests to let certain sites send browser notifications.

Whois records show that the domain was created on May 16. That’s one day after the WP Live Chat Support developers released version 8.0.27, which fixed the vulnerability. Shrotriya published a list of 47 sites he said had been hit by the exploit. While some caused malicious redirects, others didn’t and reported they were using patched versions of the plugin.

<https://arstechnica.com/?p=1512259>