A security researcher with a grudge is dropping Web 0days on innocent users

reader comments

86 with 55 posters participating

Share this story

Over the past three weeks, a trio of critical zeroday vulnerabilities in WordPress plugins has exposed 160,000 websites to attacks that allow criminal hackers to redirect unwitting visitors to malicious destinations. A self-proclaimed security provider who publicly disclosed the flaws before patches were available played a key role in the debacle, although delays by plugin developers and site administrators in publishing and installing patches have also contributed.

Over the past week, zeroday vulnerabilities in both the Yuzo Related Posts and Yellow Pencil Visual Theme Customizer WordPress plugins—used by 60,000 and 30,000 websites respectively—have come under attack. Both plugins were removed from the WordPress plugin repository around the time the zeroday posts were published, leaving websites little choice than to remove the plugins. On Friday (three days after the vulnerability was disclosed), Yellow Pencil issued a patch. At the time this post was being reported, Yuzo Related Posts remained closed with no patch available.

In-the-wild exploits against Social Warfare, a plugin used by

70,000 sites, started three weeks ago. Developers for that plugin quickly patched the flaw but not before sites that used it were hacked.

Scams and online graft

All three waves of exploits caused sites that used the vulnerable plugins to surreptitiously redirect visitors to sites pushing tech-support scams and other forms of online graft. In all three cases, the exploits came after a site called Plugin Vulnerabilities published detailed disclosures on the underlying vulnerabilities. The posts included enough proof-of-concept exploit code and other technical details to make it trivial to hack vulnerable sites. Indeed, some of the code used in the attacks appeared to have been copied and pasted from the Plugin Vulnerabilities posts.

Within hours of Plugin Vulnerabilities publishing the Yellow Pencil Visual Theme and Social Warfare disclosures, the zeroday vulnerabilities were actively exploited. It took 11 days after Plugin Vulnerabilities dropped the Yuzo Related Posts zeroday for in-the-wild exploits to be reported. There were no reports of exploits of any of the vulnerabilities prior to the disclosures.

All three of Plugin Vulnerabilities' zeroday posts came with boilerplate language that said the unnamed author was publishing them to protest "the moderators of the WordPress Support Forum's continued inappropriate behavior." The author told Ars that s/he only tried to notify developers after the zerodays were already published.

"Our current disclosure policy is to full disclose vulnerabilities and then to try to notify the developer through the WordPress Support Forum, though the moderators there… too often just delete those messages and not inform anyone about that," the author wrote in an email.

According to a blog post Social Warfare developer Warfare Plugins published Thursday, here's the timeline for March 21, when Plugin Vulnerabilities dropped the zeroday for that plugin:

> ***02:30 PM*** *(approx.) – An unnamed individual published the exploit for hackers to take advantage of. We don't know the exact time of the release because the individual has hidden the publishing time. Attacks on unsuspecting websites begin almost immediately.*
>
> ***02:59 PM*** *– WordPress discovers the publication of the vulnerability, removes Social Warfare from the WordPress.org repository, and emails our team about the issue.*
>
> ***03:07 PM*** *– In a responsible, respectable way, WordFence publishes their discovery of the publication and vulnerability, giving no details about how to take advantage of the exploit.*
>
> ***03:43 PM*** *– Every member of the Warfare Plugins team is brought up to speed, given tactical instructions, and begins taking action on the situation in each respective area: development, communications, and customer support.*
>
> ***04:21 PM*** *– A notice saying that we are aware of exploit, along with instructions to disable the plugin until patched, was posted to Twitter as well as to our website.*
>
> ***05:37 PM*** *– Warfare Plugins development team makes final code commits to patch the vulnerability and undo any malicious script injection that was causing sites to be redirected. Internal testing begins.*
>
> ***05:58 PM*** *– After rigorous internal testing, and sending a patched version to WordPress for review, the new version of Social Warfare (3.5.3) is released.*
>
> ***06:04 PM*** *– Email to all Social Warfare – Pro customers is*

sent with details of the vulnerability, and instructions on how to update immediately.

No remorse

The author said s/he scoured both Yuzo Related Posts and Yellow Pencil for security after noticing they had been removed without explanation from the WordPress plugin repository and becoming suspicious. “So while our posts could have led to exploitation, it also [sic] possible that a parallel process is happening,” the author wrote.

The author also pointed out that 11 days passed between the disclosure of the Yuzo Related Posts zeroday and the first known reports it was being exploited. Those exploits wouldn’t have been possible had the developer patched the vulnerability during that interval, the author said.

Asked if there was any remorse for the innocent end users and website owners who were harmed by the exploits, the author said: “We have no direct knowledge of what any hackers are doing, but it seems likely that our disclosures could have led to exploitation attempts. These full disclosures would have long ago stopped if the moderation of the Support Forum was simply cleaned up, so any damage caused by these could have been avoided, if they would have simply agreed to clean that up.”

The author declined to provide a name or identify Plugin Vulnerabilities other than to say it was a service provider that finds vulnerabilities in WordPress plugins. “We are trying to keep ahead of hackers, since our customers pay us to warn them about vulnerabilities in the plugins they use, and it obviously is better to be warning them before they could have been exploited instead of after.”

Whois Plugin Vulnerabilities?

The Plugin Vulnerabilities website has a copyright footer on each page that lists White Fir Designs, LLC. Whois records for pluginvulnerabilities.com and whitefirdesign.com also list the owner as White Fir Designs of Greenwood Village, Colorado. A business database search for the state of Colorado shows that White Fir Designs was incorporated in 2006 by someone named John Michael Grillot.

The crux of the author's beef with WordPress support-forum moderators, according to threads such as this one, is that they remove his posts and delete his accounts when he discloses unfixed vulnerabilities in public forums. A recent post on Medium said he was "banned for life" but had vowed to continue the practice indefinitely using made-up accounts. Posts such as this one show Plugin Vulnerabilities' public outrage over WordPress support forums has been brewing since at least 2016.

To be sure, there's plenty of blame to spread around recent exploits. Volunteer-submitted WordPress plugins have long represented the biggest security risk for sites running WordPress, and so far, developers of the open source CMS haven't figured out a way to sufficiently improve the quality. What's more, it often takes far too long for plugin developers to fix critical vulnerabilities and for site administrators to install them. Warfare Plugins' blog post offers one of the best apologies ever for its role in not discovering the critical flaw before it was exploited.

But the bulk of the blame by far goes to a self-described security provider who readily admits to dropping zerodays as a form of protest or, alternatively, as a way to keep customers safe (as if exploit code was necessary to do that). With no apologies and no remorse from the discloser—not to mention a dizzying number of buggy, poorly-audited plugins in the

WordPress repository—it wouldn’t be surprising to see more zeroday disclosures in the coming days.

This post was updated to remove incorrect details about White Fir Design.

https://arstechnica.com/?p=1490817