Ram Gall March 30, 2022

Reflected XSS in Spam protection, AntiSpam, FireWall by CleanTalk

Update – after this article was published, Denis Shagimuratov of CleanTalk reached out to us on Twitter. It appears tha they didn't receive our disclosure because our contact at the company was no longer the correct recipient for this type issue.

On February 15, 2022, the Wordfence Threat Intelligence team finished research on two separate vulnerabilities in Sp protection, AntiSpam, FireWall by CleanTalk, a WordPress plugin with over 100,000 installations. These were both reflected Cross-Site scripting vulnerabilities which could be used for site takeover if an attacker could successfully tri a site administrator into performing an action, such as clicking a link.

We initially attempted to contact CleanTalk the same day via a method that we had previously used to successfully report vulnerabilities. After we did not receive a response for over a month, we contacted the WordPress plugins tear on March 22, 2022. A patched version, 5.174.1, was made available on March 25, 2022.

All Wordfence customers, including Wordfence Premium, Wordfence Care, and Wordfence Response customers as v as Wordfence free users, are protected against any exploits targeting these vulnerabilities by the Wordfence firewall's built-in Cross-Site Scripting protection.

Description: Reflected Cross-Site Scripting
Affected Plugin: Spam protection, AntiSpam, FireWall by CleanTalk
Plugin Slug: cleantalk-spam-protect
Plugin Developer: CleanTalk
Affected Versions: <= 5.173
CVE ID: CVE-2022-28221
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Ramuel Gall
Fully Patched Version: 5.174.1

CleanTalk is a WordPress plugin designed to protect websites from spam comments and registrations. One of the features it includes is the ability to check comments for spam and present the spammy comments for deletion. The plugin uses the `column_ct_comment` function in `/lib/Cleantalk/ApbctWP/FindSpam/ListTable/Comments.ph`

display the list of spam comments, and in doing so generates links to approve, trash, or mark comments as spam us

use this parameter to perform a reflected cross-site scripting attack, which is almost identical to a vulnerability we recently covered.

The vulnerability can be used to execute JavaScript in the browser of a logged-in administrator, for instance, by trickii them into visiting a self-submitting form that sends a POST request to the site at `wp-admin/edit-comments.php?page=ct_check_spam`, with the `$_POST['page']` parameter set to malicious JavaScript.

As with any Cross-Site Scripting vulnerability, executing JavaScript in an administrator's session can be used to take over a site by adding a new malicious administrator or injecting a backdoor, among other potential methods.

Description: Reflected Cross-Site Scripting
Affected Plugin: Spam protection, AntiSpam, FireWall by CleanTalk
Plugin Slug: cleantalk-spam-protect
Plugin Developer: CleanTalk
Affected Versions: <= 5.173
CVE ID: CVE-2022-28222
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Ramuel Gall
Fully Patched Version: 5.174.1

Similar to the spam comment functionality, CleanTalk also includes a feature that checks for spammy users and presents them in a similar table for review and deletion. In this case the vulnerable function is `column_ct_username` i `/lib/Cleantalk/ApbctWP/FindSpam/ListTable/Users.php`, which uses the value of `$_REQUEST['page']` to gener links to delete potentially spammy users. As with the spam comment vulnerability, if an administrator can be tricked performing an action, it is possible to use JavaScript running in their browser to take over a site.

Timeline

February 15, 2022 – The Wordfence Threat Intelligence team finishes our investigation and verifies that the Wordfen firewall's built-in protection is sufficient to block exploit attempts. We send the full disclosure to a contact at CleanTa that we have successfully disclosed vulnerabilities to in the past.
March 22, 2022 – As we have not yet heard back from our contact, we reported the vulnerability to the WordPress plugins team.
March 25, 2022 – A patched version of the plugin, 5.174.1, becomes available.

Conclusion

In today's article, we covered two nearly identical reflected Cross-Site Scripting vulnerabilities in the Spam protection, AntiSpam, FireWall by CleanTalk plugin for WordPress. While both of these vulnerabilities require some degree of soc engineering, both could be used for site takeover.

All Wordfence users, including those running Wordfence Premium, Wordfence Care, and Wordfence Response, as we as sites still running the free version of Wordfence, are fully protected against this vulnerability.

If you believe your site has been compromised as a result of this vulnerability or any other vulnerability, we offer Incid Response services via Wordfence Care. If you need your site cleaned immediately, Wordfence Response offers the same service with 24/7/365 availability and a 1-hour response time. Both these products include hands-on support i case you need further assistance.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory them to help keep their sites protected, as this is a serious vulnerability that can lead to complete site takeover.

Comments

4 Comments

Bianca *
March 30, 2022

In my opinion, the non responsiveness from authors on vulnerability issues like these, is an instant reason for me not to install any product by them in the future. As I find it really telling.

Lizzy McNett *
March 30, 2022
7:06 am

Thank you for the info. I have been having problems with attacks, and since I read this article it makes sense, and have corrected the problem.

Mary H *
April 1, 2022
8:32 pm

According to my tests at https://observatory.mozilla.org/ and https://www.upguard.com/, this has NOT been patched. I have the patched version loaded on 29 of my sites. Until today, I had never used either of those tools. On the support thread for CleanTalk at WordPress.org, someone else posted today that they were contacted by their host because they were running an insecure plugin. It was CleanTalk's patched version. Not happy.

Ram Gall *
April 5, 2022
1:47 pm

Hi Mary,

I can assure you that the patched version 5.174.1 has corrected the issue we found in the CleanTalk plugin. These types of external security scanners do not detect WordPress-specific vulnerabilities and provide generic security recommendations. In this case https://observatory.mozilla.org/ recommends a content security policy that cannot practically be implemented on WordPress sites, and it appears that Upguard has similar recommendations. In other words, it's not currently possible to pass these assessments with a normal WordPress site, but they also won't tell you if you're genuinely vulnerable.

Wordfence Response
Wordfence Central

Premium Support

Security
CVE Request Form

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

By checking this box I agree to the terms of service and privacy policy.*

SIGN UP