

## High Severity Vulnerability Patched in Real-Time Find and Replace Plugin

On April 22, 2020, our Threat Intelligence team discovered a vulnerability in Real-Time Find and Replace, a WordPress plugin installed on over 100,000 sites. This flaw could allow any user to inject malicious Javascript anywhere on a site if they could trick a site's administrator into performing an action, like clicking on a link in a comment or email.

the vulnerability to them. This is considered a high-severity security issue, therefore we strongly recommend an immediate update to the latest version available, which at the time of writing is version 4.0.2.

Both Wordfence Premium and Free Wordfence users are protected from XSS attempts against this vulnerability by the Wordfence firewall's built-in XSS protection.

Description: Cross-Site Request Forgery to Stored Cross-Site Sc Affected Pulgin Bail Time Find a Regione Plugin Stug: real-time find-and-replace Affected Versions: ~3.9 CVES DCW: 28 (50) 13641 CVES Soore: 28 (51) 1304 CVE

Real-Time Find and Replace provides functionality to dynamically replace any HTML content on WordPress sites with new content without permanently changing the source content. The replacement data loads immediately before it is delivered to the user's browser. The plugin is very easy to use due to its limited functionality.

To provide this functionality, the plugin registers a sub-menu page tied to the function far options page with a capability requirement to "activate plugins."

```
function far_add_pages() {
    Spage = add_submenu_page( 'tools.php', 'Real-Time Find and Replace', 'Real-Time Find and Replace', 'activate_plugin add_action('admin_print_scripts'Spage', 'far_admin_scripts');

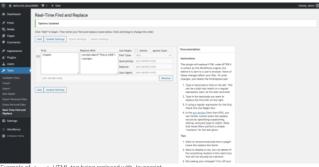
4
```

The far\_options\_page function contains the core of the plugin's functionality for adding new find and replace rules. Unfortunately, that function failed to use nonce verification, so the integrity of a request's source was not verified during rule update, resulting in a Cross-Site Request Forgery vulnerability.

```
function far_options_page() {
   if ( isset( $_POST['setup-update'] ) ) {
      $_POST = stripslashes_deep( $_POST );
}
                                 // If atleast one find has been submitted if ( isset ( \mbox{\tt SPOST['farfind']} ) & is, array( \mbox{\tt SPOST['farfind']} ) ( foreach ( \mbox{\tt SPOST['farfind']} as \mbox{\tt Skey} \Rightarrow \mbox{\tt Sfind}) (
4
```

Any attacker capable of tricking a site owner into executing an unwanted action could replace any content or HTML on a vulnerable site with new content or malicious code. This replacement code or content would then execute anytime a user navigated to a page that contained the original content.

An attacker could use this vulnerability to replace a HTML tag like <head> with malicious Javascript. This would cause the malicious code to execute on nearly every page of the affected site, as nearly all pages start with a <head> HTML tag for the page header, creating a significant impact if successfully exploited. The malicious code could be used to inject a new administrative user account, steal session cookies, or redirect users to a malicious site, allowing attackers the ability to obtain administrative access or to infect innocent visitors browsing a compromised site.



Example of <head> HTML tag being replaced with Javascript

In the most up to date version, a nonce has been added along with a  ${\tt check\_admin\_referer}$  nonce verification function to ensure the legitimacy of the source of a request.



## Disclosure Timeline

April 22, 2020 – Initial discovery and analysis of vulnerability. We verify the Wordfence built-in XSS firewall rule is sufficient. Initial outreach to plugin developer.

April 22, 2020 8:51 AM UTC – Developer responds confirming appropriate inbox.

April 22, 2020 9:34 AM UTC – We provide the full disclosure.

We see the sufficient of the part of the p

April 22, 2020 1:30 PM UTC – We receive notification that patch has been released.

## Conclusion

In today's post, we detailed a Cross-Site Request Forgery flaw in the Real-Time Find and Replace plugin. This flaw has been fully patched in version 4.0.2. We recommend that users update to the latest version, which is available  $immediately. \ Sites \ runnin \underline{\textit{9} \ Wordfence \ Premium,}} \ as \ well \ as \ sites \ using \ the \ free \ version \ of \ Wordfence, \ are \ protected \ from$ Cross-Site Scripting attacks against this vulnerability due to the Wordfence firewall's built-in protection. If you are aware of a friend or colleague using this plugin, we recommend you forward this security advisory to them as soon as possible to help secure their site. Did you enjoy this post? Share it!

Comments

No Comments

Breaking WordPress Security Research in your inbox as it happens.

you@example.com			
By checking this box I:	agree to the terms of service and p	rivacy policy.*	
SIGN UP			
Our bus	siness hours are 9am-8pm ET, 6am-5pn	n PT and 2pm-1am UTC/GMT excluding	g weekends and holidays.
	Response customers receive 24-hour	support, 365 days a year, with a 1-hou	r response time.
	Terms of Service	Privacy Policy	
	CCPA Privacy Noti	ce	
	¥	f • 0	
Products	Support	News	About
		Blog	About Wordfence
Wordfence Free	<u>Documentation</u>	BIOU	
Vordfence Premium	Learning Center	In The News	Careers
Nordfence Premium Nordfence Care Nordfence Response			Careers Contact Security
Nordfence Premium Nordfence Care	Learning Center Free Support Premium Support	In The News	Careers Contact
Nordfence Premium Nordfence Care Nordfence Response	Learning Center Free Support Premium Support Stay Updated	In The News Vulnerability Advisories	Careers Contact Security CVE Request Form
Nordfence Premium Nordfence Care Nordfence Response	Learning Center Free Support Premium Support Stay Updated	In The News	Careers Contact Security CVE Request Form
Nordfence Premium Nordfence Care Nordfence Response	Leaming Center Free Support Premium Support  Stay Updated Sign up for news and upda	In The News Vulnerability Advisories	Careers Contact Security CVE Request Form
Nordfence Premium Nordfence Care Nordfence Response	Learning Center Free Support Premium Support  Stay Updated Sign up for news and upda professionals.  you@example.com	In The News Vulnerability Advisories Vulnerability Advisories tes from our panel of experienced	Careers Contact Security CVE Request Form
Nordfence Premium Nordfence Care Nordfence Response	Learning Center Free Support Premium Support  Stay Updated Sign up for news and upda professionals.  you@example.com	In The News Vulnerability Advisories	Careers Contact Security CVE Request Form

© 2012-2022 Defiant Inc. All Rights Reserved