Vulnerability Reported in All in One SEO Pack by @martinibuster

A cross-site scripting vulnerability has been reported by the WPScan Vulnerability Database. The vulnerability was discovered by RipsTech security software company on October 25, 2018. It is unclear whether the vulnerability has been patched.

Cross-Site Scripting Vulnerability

A cross-site scripting vulnerability (XSS) is a type of vulnerability that allows an attacker to insert a code into a web page. The code compromises the web page and allows the attacker to gain various levels of access to the website and/or website database.

This is a screenshot from the RipsTech.com website showing the lines of code that contain the vulnerability.

Who Does the All in One SEO Pack Vulnerability Affect?

The All in One SEO Pack vulnerability affects websites that have at least a contributor level access enabled. The attacker must first gain access to at least the contributor level account in order to proceed with the XSS attack. It may be useful to make sure all user passwords from contributor level on up are secure.

How Does the Vulnerability Work?

Once an attacker has access to at least a contributor level user account, they can insert scripts into posts that then perform a variety of actions that can further compromise the website.

This is how the RipsTech site describes the vulnerability:

> *"An attacker is able to inject arbitrary JavaScript code into blog posts he creates and publishes. If an administrator opens a malicious blog post, evil JavaScript code executes which compromises the target server."*

Is there a Patch for the Vulnerability?

A patch is an update to software that closes a vulnerability. When a WordPress plugin fixes a vulnerability, they issue a patch and note it in what's called a *changelog*.

A changelog is a log of all the changes contained in a WordPress Plugin update. It's a good idea to review the changelog before updating because it sometimes contains important information.

For example, some plugin authors will try to minimize that a plugin contains a vulnerability and will not formally communicate to their users how urgent it is to update the plugin. Some plugin authors will only make a reference to a "security fix" within their changelog.

That said, many plugin authors include an explanation. So it's good to read the changelog to understand what's being changed.

According to the RipsTech security software company, All in One SEO Pack have not responded to affirm that a patch has

been issued.

RipsTech reports that the vendor replied on October 25, 2018 that they will investigate the vulnerability. Almost a month later, on November 22, 2018, the security company contacted the vendor again. According to RipsTech All in One SEO Pack did not send a reply.

All in One SEO Pack hosts a changelog on their website here.

According to their changelog there have been no security

updates.

The most recent changelog and the dates going back to the discovery of the vulnerability do not indicate that a security patch was issued for the XSS vulnerability.

What Should You Do?

In order for an attacker to exploit this vulnerability they would have to take control of a user account with at least the minimum level of contributor.

So it may be useful to tighten up all passwords to make sure none can be easily guessed. That will help prevent a hacker from guessing a password.

If you are not already using a WordPress security plugin like Sucuri Security or WordFence, you may wish to consider using one. These kinds of security plugins can slow down password guessing hack attacks.

There was no follow up from All in One SEO Pack to the RipsTech site if their investigation revealed an actual vulnerability or not. So at this point there is no official denial or acknowledgement of a vulnerability.

View the original announcement at RipsTech:
Click the link below to visit their "Security Calendar" then click on the number 4 in the top row. That will spawn a pop up with all the details.
https://www.ripstech.com/php-security-calendar-2018/

Read the announcement at the WPScan Vulnerability Database
https://wpvulndb.com/vulnerabilities/9159

More Resources

Images by Shutterstock, Modified by Author
Screenshots by Author, Modified by Author

Subscribe to SEJ

Get our daily newsletter from SEJ's Founder Loren Baker about the latest news in the industry!

http://tracking.feedpress.it/link/13962/10894197