7 WordPress Vulnerabilities Discovered – What You Need to Know by @martinibuster

WordPress released two updates to fix multiple vulnerabilities. The vulnerabilities have existed since version 3.7. If you have WordPress 5.0, update to 5.0.1. If you want to remain with WordPress 4, update to version 4.9.9. The update may cause backward compatibility issues with some plugins and themes. But that's less trouble than being hacked.

The WordPress Vulnerabilities

There are seven issues that allow hackers to obtain access to a site.

1. Authenticated File Delete
2. Authenticated Post Type Bypass
3. PHP Object Injection via Meta Data
4. Authenticated Cross-Site Scripting (XSS)
5. Cross-Site Scripting (XSS) that could affect plugins
6. User Activation Screen Search Engine Indexing
   Exposes emails and default generated passwords to search engines
7. File Upload to XSS on Apache Web Servers

Versions of WordPress Affected

These seven vulnerabilities affect versions 3, 4, and 5 of WordPress. All WordPress users are recommended to upgrade to WordPress versions 4.9.9 or 5.0.1.

What the WordPress official announcement noted:

> *WordPress versions 5.0 and earlier are affected by the*

> *following bugs, which are fixed in version 5.0.1. Updated versions of WordPress 4.9 and older releases are also available, for users who have not yet updated to 5.0.*

Backwards Compatibility Issues

A backward compatibility issue is a problem that causes certain functions to no longer work. For example, the <form> element has been disabled for authors to use. This could affect how plugins function unless they too are updated in order to function in the new environment.

Another issue affecting the upgraded versions of WordPress is the inability to upload CSV files. According to a full time WordPress contributor, it was necessary to disable the upload of CSV files.

CSV files are temporarily disabled on WordPress until a suitable bug fix is created.

Should You Upgrade?

Yes, you should upgrade immediately. Many WordPress sites are upgrading automatically. If you are not upgraded to 4.9.9 or to 5.0.1 at this time, then you should initiate an update right away. Updating is easy, just go to your WordPress dashboard and there should be an announcement.

How Bad are the Vulnerabilities?

The vulnerabilities should be taken seriously. Staying with an obsolete version of WordPress could possibly expose you to

a hacking event. One of the WordPress contributors expressed that sentiment in the comment sections of the official announcement:

Read the official WordPress announcement here.

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/13962/10904548