WordPress Announces Another Security Release: Version 7.1.4 via @sejournal, @martinibuster

WordPress announced a security release, version 7.1.4, intended to fix 22 vulnerabilities, including a potentially dangerous weakness in the update process and numerous stored cross-site scripting vulnerabilities.

This release contains three significant kinds of fixes:

1. The WordPress update process itself was vulnerable.
A race condition could allow remote code execution during the upgrade window. This is arguably the most consequential of the discovered flaws that is being patched because these kinds of vulnerabilities can lead to a full site takeover. The official announcement however does not offer information about the conditions necessary to exploit it.

2. The vulnerabilities extend across WordPress's editing and interactive functionality.
Multiple issues affect the Interactivity API, blocks, the Customizer, and administrative interfaces with some of involving unauthorized disclosure of information. Many of these exploits require Contributor-level access or higher, which minimizes the likelihood of exploitation. but some involve.

3. The security problems affect recent and older WordPress versions.
This security release fixes vulnerabilities that date back as

far as WordPress 4.7, with the number of applicable vulnerabilities varying by version. This reflects how central some of the affected components are within the WordPress core itself.

WordPress Fixes Remote Code Execution Risk In Its Update Process

Security researcher Umut Bayram discovered a race condition affecting WordPress core updates. Under certain conditions, this vulnerability could lead to remote code execution (RCE). Remote code execution (RCE) is a security vulnerability that enables an attacker to run malicious commands or software on a website's server from a remote location. Depending on the attacker's level of access, this can lead to anything from stolen data to a complete website takeover.

The announcement rightfully leaves out many details of the vulnerabilities, likely to make it harder to exploit. So it's not known what access or server conditions are necessary to exploit the update race condition or whether authentication is required.

Read more: WordPress 7.1.4 Security Release

Featured Image by Shutterstock/Luis Molinero

https://www.searchenginejournal.com/wordpress-announces-another-security-release-version-7-1-4/594798/