Hackers are exploiting a critical flaw affecting >350,000 WordPress sites

reader comments

58 with 41 posters participating

Share this story

Hackers are actively exploiting a vulnerability that allows them to execute commands and malicious scripts on Websites running File Manager, a WordPress plugin with more than 700,000 active installations, researchers said on Tuesday. Word of the attacks came a few hours after the security flaw was patched.

Attackers are using the exploit to upload files that contain webshells that are hidden in an image. From there, they have a convenient interface that allows them to run commands in plugins/wp-file-manager/lib/files/, the directory where the File Manager plugin resides. While that restriction prevents hackers from executing commands on files outside of the directory, hackers may be able to exact more damage by uploading scripts that can carry out actions on other parts of a vulnerable site.

NinTechNet, a website security firm in Bangkok, Thailand, was among the first to report the in-the-wild attacks. The post said that a hacker was exploiting the vulnerability to upload a script titled hardfork.php and then using it to inject code into the WordPress scripts /wp-admin/admin-ajax.php and /wp-

includes/user.php.

Backdooring vulnerable sites at scale

In email, NinTechNet CEO Jerome Bruandet wrote:

> *It's a bit too early to know the impact because when we caught the attack, hackers were just trying to backdoor websites. However, one interesting thing we noticed is that attackers were injecting some code to password-protect the access to the vulnerable file (connector.minimal.php) so that other groups of hackers could not exploit the vulnerability on the sites that were already infected.*
>
> *All commands can be run in the /lib/files folder (create folders, delete files etc), but the most important issue is that they can upload PHP scripts into that folder too, and then run them and do whatever they want to the blog.*
>
> *So far, they are uploading "FilesMan", another file manager often used by hackers. This one is heavily obfuscated. In the next few hours and days we'll see exactly what they will do, because if they password-protected the vulnerable file to prevent other hackers to exploit the vulnerability it is likely they are expecting to come back to visit the infected sites.*

Fellow website security firm Wordfence, meanwhile, said in its own post that it had blocked more than 450,000 exploit attempts in the past few days. The post said that the attackers are trying to inject various files. In some cases, those files were empty, most likely in an attempt to probe for vulnerable sites and, if successful, inject a malicious file later. Files being uploaded had names including hardfork.php, hardfind.php, and x.php.

“A file manager plugin like this would make it possible for an attacker to manipulate or upload any files of their choosing directly from the WordPress dashboard, potentially allowing them to escalate privileges once in the site’s admin area,” Chloe Chamberland, a researcher with security firm Wordfence, wrote in Tuesday’s post. “For example, an attacker could gain access to the admin area of the site using a compromised password, then access this plugin and upload a webshell to do further enumeration of the server and potentially escalate their attack using another exploit.”

52% of 700,000 = potential for damage

The File Manager plugin helps administrators manage files on sites running the WordPress content management system. The plugin contains an additional file manager known as elFinder, an open source library that provides the core functionality in the plugin, along with a user interface for using it. The vulnerability arises from the way the plugin implemented elFinder.

“The core of the issue began with the File Manager plugin renaming the extension on the elFinder library’s connector.minimal.php.dist file to .php so it could be executed directly, even though the connector file was not used by the File Manager itself,” Chamberland explained. “Such libraries often include example files that are not intended to be used ‘as is’ without adding access controls, and this file had no direct access restrictions, meaning the file could be accessed by anyone. This file could be used to initiate an elFinder command and was hooked to the elFinderConnector.class.php file.”

The developers of File Manager credited researches Ville Korhonen and Seravo with discovering and first reporting the vulnerability. The researchers, who said they found the

vulnerability as part of their regular “WordPress upkeep service,” published their own writeup here.

Sal Aguilar, a contractor who sets up and secures WordPress sites, took to Twitter to warn of attacks he’s seeing.

“Oh crap!!!” he wrote. “The WP File Manager vulnerability is SERIOUS. Its spreading fast and I’m seeing hundreds of sites getting infected. Malware is being uploaded to /wp-content/plugins/wp-file-manager/lib/files.”

The security flaw is in File Manager versions ranging from 6.0 to 6.8. Statistics from WordPress show that currently about 52 percent of installations are vulnerable. With more than half of File Manager’s installed base of 700,000 sites vulnerable, the potential for damage is high. Sites running any of these versions should updated to 6.9 as soon as possible.

Updated to add fourth-to-last paragraph.

https://arstechnica.com/?p=1702887