Open source bug poses threat to sites running multiple CMSes

reader comments

33 with 24 posters participating

Share this story

Websites running the Drupal, Joomla, or Typo3 content-management systems are vulnerable to attacks that could possibly execute malicious code until administrators install just-released patches, developers and security researchers warned.

The vulnerability resides in the PharStreamWrapper, a PHP component developed and open-sourced by CMS maker Typo3. Indexed as CVE-2019-11831, the flaw stems from a path-traversal bug that allows hackers to swap a site's legitimate phar archive with a malicious one. A phar archive is used to distribute a complete PHP application or library in a single file, in much the way a Java archive file bundles many Java files into a single file.

In an advisory published Wednesday, Drupal developers rated the severity of the vulnerability affecting their CMS as moderately critical. That's well below the highly critical rating of a recent Drupal vulnerability and earlier remote-execution flaws that took on the name "Drupalgeddon." Still, the vulnerability represents enough of a risk that administrators should patch it as soon as possible.

“The nature of the [pharStreemWarapper] vulnerability makes it context dependent,” Daniel le Gall, a researcher who discovered the vulnerability, told Ars. “I found this vulnerability on Drupal, and that’s the only platform where I assessed the severity. I’m currently talking with Drupal to make it ‘critical’ instead of ‘moderately critical,’ but the final decision is in their hands.”

A researcher at SCRT SA in Switzerland, le Gall said his own calculus using Drupal’s published severity rating method led him to the determination the vulnerability should be rated critical. Still, he agreed that CVE-2019-11831 was well below the threshold of previous Drupal bugs, which could be exploited by unprivileged end users visiting a vulnerable site.

“For a default Drupal [site] without plugins, it requires [the site] to have a user with the ‘Administer theme’ right, which is a high prerequisite,” he said. That means that an attacker would have to have limited administrator privileges, such as those given to marketing people or graphic designers.

“However, some community modules might be vulnerable because of this flaw in the Drupal Core,” he added. “Once these privileges are obtained, the flaw is pretty easy to exploit, however, and effectively leads to remote code execution.”

Joomla developers, meanwhile, issued their own advisory on Wednesday that rated the severity low. Typo3 developers didn’t provide a severity rating for their own CMS.

Sites that run:

- Drupal 8.7 should update to 8.7.1
- 8.6 or earlier should update to 8.6.16
- 7 should update to 7.67

On Joomla, the flaw affects versions 3.9.3 through 3.9.5. The fix is available in 3.9.6.

Typo3 CMS users should either upgrade to PharStreamWapper versions v3.1.1 and v2.1.1 manually or ensure Composer dependencies are raised to those versions.

https://arstechnica.com/?p=1502725