Millions of websites threatened by highly critical code-execution bug in Drupal

reader comments

32 with 28 posters participating

Share this story

Millions of sites that run the Drupal content management system run the risk of being hijacked until they're patched against a vulnerability that allows hackers to remotely execute malicious code, managers of the open source project warned Wednesday.

CVE-2019-6340, as the flaw is tracked, stems from a failure to sufficiently validate user input, managers said in an advisory. Hackers who exploited the vulnerability could, in some cases, run code of their choice on vulnerable websites. The flaw is rated highly critical.

"Some field types do not properly sanitize data from non-form sources," the advisory stated. "This can lead to arbitrary PHP code execution in some cases."

For a site to be vulnerable, one of the following conditions must be met:

- It has the Drupal 8 core RESTful Web Services (rest) module enabled and allows PATCH or POST requests or
- It has another Web-services module enabled, such as JSON:API in Drupal 8, or Services or RESTful Web

Services in Drupal 7

Project managers are urging administrators of vulnerable websites to update at once. For sites running version 8.6.x, this involves upgrading to 8.6.10 and sites running 8.5.x or earlier upgrading to 8.5.11. Sites must also install any available security updates for contributed projects after updating the Drupal core. No core update is required for Drupal 7, but several Drupal 7 contributed modules do require updates.

Popular hacking target

Drupal is the third most-widely used CMS behind WordPress and Joomla. With an estimated 3 percent to 4 percent of the world's billion-plus websites, that means Drupal runs tens of millions of sites. Critical flaws in any CMS are popular with hackers, because the vulnerabilities can be unleashed against large numbers of sites with a single, often-easy-to-write script.

In 2014 and again last year, hackers wasted no time exploiting extremely critical code-execution vulnerabilities shortly after they were fixed by Drupal project leaders. Last year's "Drupalgeddon2" vulnerability was still being exploited six weeks after it was patched, an indication that many sites that run on Drupal failed to heed the urgent advice to patch.

At the time this post was going live, there were no reports of the latest Drupal vulnerability being actively exploited in the wild. This is obviously subject to change. This post will be updated if new information becomes available.

https://arstechnica.com/?p=1462289