Critical Drupal Core Vulnerability – Upgrade Now by @martinibuster

A Drupal core vulnerability was announced on the official Drupal website. This is called the **SA-CORE-2018-004** vulnerability. This vulnerability allows a remote attacker to execute code on a Drupal website through "multiple attack vectors." The official Drupal site recommends upgrading to the most recent versions of Drupal 7 or 8. Attacks based on this vulnerability have not yet been observed in the wild. So it's important to get ahead of it and update soon.

What is a Remote Code Execution Vulnerability?

A remote code execution vulnerability is a security hole that allows an attacker to run code on a web site. By running the code the attacker could gain access to the website, server and/ or database.

Where Can a Patch be Downloaded?

Drupal has released updated versions on their website. However, these patches will only work if you have already upgraded from the previously reported vulnerability, SA-CORE-2018-002, that was announced two weeks ago.

Here is the recommended solution from Drupal:

- *If you are running 7.x, upgrade to* ***Drupal 7.59****.*

- *If you are running 8.5.x, upgrade to Drupal 8.5.3.*

- *If you are running 8.4.x, upgrade to Drupal 8.4.8. (Drupal 8.4.x is no longer supported and we don't normally provide security releases for unsupported minor releases. However, we are providing this 8.4.x release so that sites can update as quickly as possible. You should update to 8.4.8 immediately, then update to 8.5.3 or the latest secure release as soon as possible.)*

> *If you are unable to update immediately, or if you are running a Drupal distribution that does not yet include this security release, you can attempt to apply the patch below to fix the vulnerability until you are able to update completely:*

What if You Don't Have the SA-CORE-2018-002 Patch?

According to Drupal.org your site may already be affected. Here is what it says:

> *The security team is now aware of automated attacks attempting to compromise Drupal 7 and 8 websites using the vulnerability reported in SA-CORE-2018-002. Due to this, the security team is increasing the security risk score of that issue to 24/25*
>
> ***Sites not patched by Wednesday, 2018-04-11 may be compromised.** This is the date when evidence emerged of automated attack attempts. It is possible targeted attacks occurred before that.*

Find more details about today’s SA-CORE-2018-004 vulnerability here

Images by Shutterstock, modified by Author

http://tracking.feedpress.it/link/13962/8969709