Tonga National Computer Emergency Response Team

Drupal- Remote Code Execution Vulnerability

Drupal is popular, free and open-source content management software (CMS), it is also a platform for web content management among global enterprises, governments, higher education institutions, and NGOs. Flexible and highly scalable, Drupal publishes a single web site or shares content in multiple languages across many devices. The Drupal security team have now released a critical update to address an unauthenticated remote code execution vulnerability in Drupal core.

How the attack works:

A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being compromised.

For your information a local website in Tonga has been compromised and we suspect that it was due to this vulnerability.

You are also adviced to take caution when using various plugins for any of the CMS sites as these are often avenues of attacks.

Solution:

Upgrade to the most recent version of Drupal 7 or 8 core.

- Make sure to always do a backup of your site before applying update patches
- 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 they don't normally provide security releases for unsupported minor releases. However, they are providing this 8.4.x release so that sites can be updated 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.)

Reference:

- https://www.tenable.com/blog/critical-drupal-core-vulnerability-what-you-need-to-know
- https://www.drupal.org/sa-core-2018-002

- https://www.bleepingcomputer.com/news/security/hackers-dont-give-site-owners-time-to-patch-start-exploiting-new-drupal-flaw-within-hours/
- https://www.drupal.org/drupal-security-team/security-risk-levels-define

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.to
web: www.cert.to