Alert – Drupal 7.x Vulnerabilities

Description

- Drupal security team discovered a highly critical remote code execution vulnerability, dubbed **Drupalgeddon2,** in its CMS software that could allow attackers to completely take over vulnerable websites. Short after it was publicly released, hackers started exploiting it.
- **Private file access bypass**- Moderately critical, when using Drupal's private file system, Drupal will check to make sure a user has access to a file before allowing the user to view or download it.

Impact of the vulnerabilities

- **Drupalgeddon2** vulnerability allows remote attacker to execute malicious code on Drupal installations CMS without requesting any authentication. As Checkpoint researchers said, an attacker could potentially inject a malicious payload into the internal form structure of Drupal, execute it without user authentication and carry out a full site takeover.
- **Private File Access bypass,** Drupal fails to check under certain conditions in which one module is trying to grant access to the file and another is trying to deny to an access bypass vulnerability.

Vulnerable versions

- Drupalgeddon2 affects all versions of Drupal from 6 to 8.
- Private File Access bypass affects Drupal 7.x

Solution: Rw-CSIRT is strongly recommending users to:

To patch the vulnerability:

- Upgrade to Drupal 8.6.1 which is the latest version.

Affected users should:

Affected users should contact RW-CSIRT: Call; 4045 or write to security@rdb.rw to help for analyzing the source of the incident and recommendation.

References:

- https://thehackernews.com/2018/04/drupal-rce-exploit-code.html
- https://www.drupal.org/sa-core-2018-002
- https://blog.securityevaluators.com/critical-remote-code-execution-vulnerability-found-in-drupal-cve-2018-7600-162f0a863f4

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of "early *Detection*, *Prevention*, *Response* to incidents and *Reduce* Vulnerability" and raise cyber security awareness in public.