Alert – Drupal Core - Multiple Vulnerabilities - SA-CORE-2018-006

Description

Multiple vulnerabilities have been discovered in Drupal core module, the most severe of which could allow for remote code execution. The remote code execution vulnerability exists within the default Drupal mail system because of improper sanitization for shell arguments, which could result in a website being completely compromised. Details of the vulnerabilities are as follows:

- In some conditions, content moderation fails to check users access to use certain transitions, leading to an access bypass.
- External URL injection through URL aliases could allow for open redirect.
- Anonymous Open Redirect if a user clicks on a specially crafted URL using the destination query string.
- Injection in DefaultMailSystem::mail() due to variables not being sanitized for shell arguments could allow for Remote Code Execution.
- The Contextual Links module did not sufficiently validate requested contextual links. When exploited this vulnerability could allow for Remote Code Execution.

Risk

All Government and Business entities the risk is **High.**

Impact of the vulnerability

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

Vulnerable versions

- Drupal Core versions prior to 7.60, 8.6.2, and 8.5.8.

Solution: Rw-CSIRT is strongly recommending users to:

- Apply appropriate patches provided by Drupal to vulnerable systems immediately after appropriate testing.
- Ensure no unauthorized system changes have occurred before applying patches.
- Run all software as a non-privileged user to diminish effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.
- Drupal version 8.4.x and earlier sites should be migrated to supported Drupal versions as soon as possible after patches are applied.

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

References:

https://www.us-cert.gov/ncas/current-activity/2018/10/18/Drupal-Releases-Security-Updates
https://www.drupal.org/sa-core-2018-006

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.