The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/18/2019

SUBJECT:
Multiple Vulnerabilities in Drupal Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities has been discovered in the Drupal core module, the most severe of which could allow for arbitrary code execution. Drupal is an open source content management system (CMS) written in PHP. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary 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.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Drupal Core versions prior to 7.66, 8.6.15 and 8.5.15

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Drupal core module, the most severe of which could allow for arbitrary code execution. The arbitrary code execution vulnerability exists due to a lack of proper data sanitization in some fields, which could result in a website being completely compromised. Details of the vulnerabilities are as follows:

- Validation messages were not escaped when using the form theme of the PHP templating engine which, when validation messages may contain user input, could result in an XSS. (CVE-2019-10909)
- Service IDs derived from unfiltered user input could result in the execution of any arbitrary code, resulting in possible remote code execution. (CVE-2019-10910)
- This fixes situations where part of an expiry time in a cookie could be considered part of the username, or part of the username could be considered part of the expiry time. An attacker could modify the remember me cookie and authenticate as a different user. (CVE-2019-10911)
- jQuery 3.4.0 includes a fix for some unintended behavior when using jQuery.extend(true, {}, ...). If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

RECOMMENDATIONS:
The following actions should be taken:

- 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 8.5.x and earlier sites should be migrated to supported Drupal versions as soon as possible after patches are applied.

REFERENCES:
Drupal:
https://www.drupal.org/sa-core-2019-005
https://www.drupal.org/sa-core-2019-006