**Vulnerability Report**

**Name**: Prasad Jadhav

**Vulnerability Title:** Drupal Core Critical RCE Vulnerability (SA-CORE-2018-002)

**Plugin ID:** 1.3.6.1.4.1.25623.1.0.108438

**CVE ID:** CVE-2018-7600

**Host Scanned:** 192.168.1.82 (DC-1)

**Tool Used:** OpenVAS (Greenbone Vulnerability Manager)

**Scan Date:** May 5, 2025 – 02:18 AM

**1. Description:** This vulnerability, known as **Drupalgeddon 2**, is a remote code execution (RCE) flaw in multiple versions of the Drupal content management system. It arises from improper input validation in the form rendering and AJAX callback systems. By sending specially crafted HTTP POST requests, an attacker can inject and execute arbitrary PHP code without any authentication. In the test case, the attacker successfully executed the printf function to return the test string v\_mYntmTEPGtEamj, confirming code execution.

**2. Risk Summary**

* **Risk Factor:** Critical
* **CVSS v3.0 Base Score:** 9.8
* **Attack Vector:** Network
* **Impact:** Complete system compromise, remote code execution
* **Exploitable Remotely:** Yes
* **Authentication Required:** No

**3. Affected Software/Services:**

* Drupal Core 6.x and earlier
* Drupal 7.x prior to 7.58
* Drupal 8.2.x and earlier
* Drupal 8.3.x prior to 8.3.9
* Drupal 8.4.x prior to 8.4.6
* Drupal 8.5.x prior to 8.5.1

**4. Remedies:**

Apply official security updates from Drupal to the following minimum versions:

* Drupal 7.58
* Drupal 8.3.9
* Drupal 8.4.6
* Drupal 8.5.1 or newer

Patches are available on the Drupal project site.

**5. Recommendations:**

* Immediately upgrade to a secure version of Drupal as listed above.
* Take the affected system offline if it is public-facing until patched.
* Check logs for indicators of compromise or exploitation attempts.
* Conduct a file integrity check to detect unauthorized changes.
* Implement WAF rules to block suspicious POST payloads targeting Drupal endpoints.
* Regularly monitor vulnerability disclosures related to web CMS platforms.

**6. References:**

* Drupal SA-CORE-2018-002
* CVE-2018-7600 - NVD
* Drupal Official Releases
* Checkpoint Research - Drupalgeddon 2
* CISA KEV Catalog