



**State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory**

**June 19, 2015**

*The following cyber advisory was issued by the State of Alaska and was 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.*

**ADVISORY NUMBER:  
SA2015-067**

**DATE(S) ISSUED:  
06/19/2015**

**SUBJECT:  
Multiple Vulnerabilities in Drupal Could Allow for Security Bypass**

**OVERVIEW:  
Multiple vulnerabilities have been discovered in Drupal core modules. Drupal is an open source content management system (CMS) written in PHP.**

**Successful exploitation of these vulnerabilities could allow an unauthorized user to hijack other user accounts - including ones with administrative privileges, allow for user redirection to potentially malicious sites, or disclose private information.**

**THREAT INTELLIGENCE  
There are currently no known exploits in the wild.**

**SYSTEM AFFECTED:**

- Drupal core 6.x versions prior to 6.36
- Drupal core 7.x versions prior to 7.38

**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:  
Drupal core modules are prone to multiple vulnerabilities. These vulnerabilities are as follows:**

- User impersonation/access bypass in the OpenID module (CVE-2015-3234)
- Open redirect in Field UI and Overlay modules (CVE-2015-3232, CVE-2015-3233)
- Information disclosure in the Render cache system (CVE-2015-3231)

Successful exploitation of these vulnerabilities could allow an unauthorized user to hijack other user accounts - including ones with administrative privileges, allow for user redirection to potentially malicious sites, or disclose private information.

#### RECOMMENDATIONS:

We recommend the following actions be taken:

- Update Drupal core to the latest version, after appropriate testing.
- Run all software as a non-privileged user to diminish effects of a successful attack.
- Limit user account privileges to those required only.

#### REFERENCES:

Drupal:

<https://www.drupal.org/SA-CORE-2015-002>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3231>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3232>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3233>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3234>