



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

March 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:
SA2015-031**

**DATE(S) ISSUED:
03/19/2015**

**SUBJECT:
Vulnerabilities in Drupal Could Allow for Security-Bypass and Phishing Attacks**

OVERVIEW:
A vulnerability has been reported in the Drupal core that could allow for phishing attacks. Drupal is an open source content management system (CMS) written in PHP. Successful exploitation of this vulnerability could result in the attacker gaining unauthorized access to the CMS and after persuading a user to follow a crafted URI, it would take the user to the attacker controlled site for phishing and other types of attacks.

THREAT INTELLIGENCE:
There is no known proof-of-concept code available at this time.

SYSTEM AFFECTED:

- Drupal core 6.x versions prior to 6.35
- Drupal core 7.x versions prior to 7.35

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:

A vulnerability has been discovered in the Drupal core that may allow an attacker to bypass security restrictions because of a failure to protect the reset password URLs. Another vulnerability that exists in the affected versions mentioned above is a failure to sanitize URLs that are supplied by the user for the “destination” parameter in a query string. This allows the attacker to place a crafted URI into the “destination” parameter and persuade a user to follow it.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Update to the latest version of Drupal core.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Drupal:

<https://www.drupal.org/SA-CORE-2015-001>

SecurityFocus:

<http://www.securityfocus.com/bid/73219>