



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

October 16, 2014

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:

SA2014-070

DATE(S) ISSUED:

10/15/2014

SUBJECT:

SQL Injection Vulnerability in Drupal could allow for Remote Code Execution

EXECUTIVE SUMMARY:

A vulnerability has been reported in Drupal 7 core that could allow for SQL injection. Drupal is an open source content management system (CMS) written in PHP. Successful exploitation of this vulnerability could result in the attacker executing arbitrary code in SQL or PHP, and possible privilege escalation. Successful exploitation could allow an attacker to control the website; view, change, delete data; or perform other activities.

THREAT INTELLIGENCE

There is not any known proof-of-concept code available at this time.

SYSTEM AFFECTED:

- Drupal core version 7 prior to 7.32

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: Low

TECHNICAL SUMMARY:

Vulnerability has been discovered in the Drupal 7 core. Specifically, this vulnerability is in the database abstraction API that sanitizes user-supplied data before using it in SQL

queries. An unauthorized attacker could create specially crafted requests resulting in arbitrary code execution (specifically PHP code) or privilege escalation. (CVE-2014-3704)

RECOMMENDATIONS:

We recommend the following actions be taken:

- Update to the latest version of Drupal core.
- If unable to update to the latest version, apply the appropriate patch found on the Drupal website to the affected site's database.inc file.
- 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-2014-005>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3704>

Security Focus:

<http://www.securityfocus.com/bid/70595>