



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

October 25, 2016

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:

SA2016-161

DATE(S) ISSUED:

10/25/2016

SUBJECT:

Multiple Vulnerabilities in Joomla Could Allow for Security Bypass

OVERVIEW:

Multiple vulnerabilities have been discovered in Joomla, the most severe of which could allow for security bypass. Joomla is an open source content management system for websites. Successful exploitation of these vulnerabilities could allow an attacker to create a user account on a website that has disabled account creation, or create a user account with escalated privileges.

THREAT INTELLIGENCE:

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

SYSTEM AFFECTED:

- Joomla prior to version 3.6.4

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Joomla! Core, the most severe of which could result in security bypass. Details of the vulnerabilities are as follows:

- Incorrect use of unfiltered data allows for users to register on a site with elevated privileges. (CVE-2016-8869)
- Inadequate checks allows for users to register on a site when registration has been disabled. (CVE-2016-8870)

Successful exploitation of these vulnerabilities could allow an attacker to create a user account on a website that has disabled account creation, or create a user account with escalated privileges.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Joomla! to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Joomla!:

<https://developer.joomla.org/security-centre.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8869>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8870>