



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

December 15, 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:

SA2015-150

DATE(S) ISSUED:

12/15/2015

SUBJECT:

Vulnerability in Joomla Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Joomla, which could result in arbitrary code execution. Joomla is an open source content management system for websites. This vulnerability can be exploited by an attacker sending a maliciously crafted packet to a vulnerable server.

Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

THREAT INTELLIGENCE:

Reports indicate that this vulnerability is being actively exploited in the wild.

SYSTEMS AFFECTED:

Joomla versions between 1.5 and 3.4.

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:

This vulnerability may be exploited by a remote attacker sending a maliciously crafted packet to a vulnerable server. Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code in the context of the application, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Joomla to vulnerable Joomla 3.X systems immediately after appropriate testing.
- Apply appropriate hotfixes provided by Joomla to vulnerable Joomla 1.5.X and 2.5.X systems immediately after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.

REFERENCES:

Joomla:

<https://www.joomla.org/announcements/release-news/5641-joomla-3-4-6-released.html>
https://docs.joomla.org/Security_hotfixes_for_Joomla_EOL_versions
<https://developer.joomla.org/security-centre/630-20151214-core-remote-code-execution-vulnerability.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8562>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8566>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8563>

Sucuri:

<https://blog.sucuri.net/2015/12/remote-command-execution-vulnerability-in-joomla.html>