



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

April 14, 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:

SA2014-030

DATE(S) ISSUED:

04/14/2014

SUBJECT:

Multiple vulnerabilities in WordPress Content Management System

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in WordPress CMS which could allow an attacker to take control of the affected system. WordPress is an open source content management system (CMS) for websites. Successful exploitation of the vulnerabilities could result in an attacker gaining un-authorized access, bypassing security restrictions, injecting scripts or HTML, and stealing cookies. Depending on the privileges gained, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

Currently we are not aware of any malicious exploitation of these vulnerabilities in the wild.

SYSTEMS AFFECTED:

- WordPress Versions 3.8 and 3.8.1 are vulnerable.

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: N/A

TECHNICAL SUMMARY:

Three vulnerabilities have been identified in WordPress CMS that could allow for an attacker to take control of the affected system.

1. An access-bypass vulnerability occurs because the CMS fails to properly validate access. This is caused due to an error in the cookie keyed hash value verification.
2. A security-bypass vulnerability has been identified in the 'publish_post' capability.
3. An HTML-injection vulnerability, as the CMS fails to sufficiently sanitize user-supplied data related to 'Plupload'.

Successful exploitation of these vulnerabilities could allow the attacker to bypass certain security restrictions, gain unauthorized access, run malicious HTML and script codes or steal cookie-based authentication credentials. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

WordPress has released WordPress 3.8.2, which corrects this issue.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Update vulnerable systems running WordPress immediately after appropriate testing.
- Review and follow WordPress hardening guidelines - http://codex.wordpress.org/Hardening_WordPress
- Confirm that the operating system and all other applications on the system running this CMS are updated with the most recent patches.
- Deploy NIDS to detect and block attacks and anomalous activity such as crafted requests containing suspicious URI sequences.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

WordPress:

<http://wordpress.org/news/2014/04/wordpress-3-8-2/>

SecurityFocus:

<http://www.securityfocus.com/bid/66765>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0165>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0166>