



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

February 9, 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:

SA2016-028

DATE(S) ISSUED:

02/09/2016

SUBJECT:

Security Update for Microsoft Office to Address Remote Code Execution (MS16-015)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office that could allow remote code execution. These vulnerabilities can be exploited when a user opens a specially crafted email or office file. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE

One cross site scripting (XSS) vulnerability (CVE-2016-0039) has been publicly disclosed. There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Office 2007, 2010, 2013, 2013 RT, 2016
- Office for Mac 2011, 2016
- Excel Viewer
- Word Viewer
- SharePoint Server 2007, 2010, 2013
- Office Web Apps 2010, 2013
- SharePoint Server 2013
- SharePoint Foundation 2013

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:

Multiple vulnerabilities exist in Microsoft Office, the most severe of which could allow remote code execution. The vulnerabilities are as follows:

- Six memory corruption vulnerabilities exist when the Office software fails to properly handle objects in member. The vulnerabilities could allow an attacker to execute remote code by luring a victim execute a malicious Microsoft Office file. (CVE-2016-0022, CVE-2016-0052, CVE-2016-0053, CVE-2016-0054, CVE-2016-0055, CVE-2016-0056)
- A cross-site scripting vulnerability exists in Microsoft SharePoint when SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. (CVE-2016-0039)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same rights as the current user. If the current user is logged on with administrative user rights an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft 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 untrusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-015.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0022>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0039>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0052>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0053>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0054>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0055>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0056>