



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

December 8, 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:

SA2015-144

DATE(S) ISSUED:

12/08/2015

SUBJECT:

Multiple Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS15-131)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office that could allow remote code execution. 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:

There is a report of one of these vulnerabilities (CVE-2015-6124) being exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Office 2007, 2010
- Microsoft Office for Mac 2011
- Microsoft Office Compatibility Pack
- Microsoft Excel 2007, 2010
- Microsoft Excel for Mac 2011, 2016
- Microsoft Excel Viewer
- Microsoft Word 2007, 2010, 2013, 2013 RT, 2016

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:**

Six vulnerabilities have been discovered in Microsoft Office. These vulnerabilities could allow remote code execution if a user previews or opens a specially crafted email message or Microsoft Office file. An attacker who successfully exploits these vulnerabilities could run arbitrary code in the context of the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Details of these vulnerabilities are as follows:

- Five memory corruption vulnerabilities exist in the way Office handles objects in memory (CVE-2015-6040; CVE-2015-6118; CVE-2015-6122; CVE-2015-6124; CVE-2015-6177)
- One Microsoft Office Remote Code Execution Vulnerability exists in the way that Microsoft Outlook parses email messages. (CVE-2015-6172)

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/MS15-131>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6040>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6118>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6122>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6124>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6172>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6177>