



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

October 22, 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:

SA2014-071

DATE(S) ISSUED:

10/22/2014

SUBJECT:

Vulnerability in Microsoft OLE Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Microsoft Windows products, excluding Server 2003. The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office file that contains an OLE object. The attack requires user interaction to succeed on Windows clients with a default configuration, as User Account Control (UAC) is enabled and a consent prompt is displayed. Successful exploitation 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:

Microsoft has reported that limited, targeted attacks have been observed attempting to exploit this vulnerability through Microsoft PowerPoint.

SYSTEM AFFECTED:

- Windows Vista
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows 8
- Windows 8.1
- Windows RT

- Windows RT 8.1

RISK:**Government:**

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

Businesses:

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

Home users: High**TECHNICAL SUMMARY:**

A vulnerability has been publicly reported in Microsoft Windows. This vulnerability can be triggered by opening a specially crafted file, via email attachment, or through the web. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted file to a user. For this attack scenario to be successful, the user must be convinced to open the specially crafted file containing the malicious Object Linking and Embedding (OLE) object. All Microsoft Office file types, as well as many other third-party file types could contain a malicious OLE object.

In a web-based attack scenario, an attacker would have to host a website that contains a specially crafted Microsoft Office file, such as a PowerPoint file, that is used in an attempt to exploit this vulnerability. In addition, compromised websites (and websites that accept or host user-provided content) could contain specially crafted content that could exploit this vulnerability. An attacker would have no method to force users to visit a malicious website. Instead, an attacker would have to persuade the targeted user to visit the website, typically by getting them to click a link that directs a web browser to the attacker-controlled website.

Successful exploitation 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.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate workarounds 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 un-trusted sources.

REFERENCES:**Microsoft:**

<https://technet.microsoft.com/library/security/3010060>

<https://support.microsoft.com/kb/3010060>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6352>

SecurityFocus:

<http://www.securityfocus.com/bid/70690>