



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

January 10, 2012

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:

SA2012-002

DATE(S) ISSUED:

01/10/2012

SUBJECT:

Vulnerability in Windows Could Allow for Remote Code Execution (MS12-005)

OVERVIEW:

A new vulnerability has been reported in a component of Microsoft Windows. Exploitation may occur if a user opens a specially crafted Microsoft Office file. This file may be received as an email attachment, or downloaded via the Web. Successful exploitation may 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.

SYSTEMS AFFECTED:

- Microsoft Windows XP
- Microsoft Vista
- Microsoft Windows 7
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

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

DESCRIPTION:

A vulnerability exists in the Windows Packager component in Microsoft Windows. This occurs when the Windows Packager fails to properly handle a Microsoft Office document embedded with malicious ClickOnce application. This vulnerability is caused due to ClickOnce application files not being included in the Windows Packager's list of unsafe file types. The Microsoft Office file may be received as an email attachment, or downloaded via the Web.

ClickOnce is a Microsoft technology, which allows programmers to create self-updating Windows-based applications. A ClickOnce application can consist of the following: Windows Presentation Foundation (.xbap), Windows Forms (.exe), console application (.exe), or Office solution (.dll). Very little user interaction is needed to install these applications. ClickOnce applications can be published in three different ways: from a web page, from a network file share, or from media such as a CD-ROM.

Successful exploitation may 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 patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms12-005>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0013>

Security Focus:

<http://www.securityfocus.com/bid/51284>