



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

April 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:

SA2012-021

DATE(S) ISSUED:

04/10/2012

SUBJECT:

Vulnerability in Windows Common Controls Could Allow Remote Code Execution (MS12-027)

OVERVIEW:

A vulnerability has been discovered in Windows Common Controls that could allow an attacker to take complete control of a vulnerable system. Windows Common Controls are a set of interfaces that enable a user to interact with an application and are used by all supported versions of the Windows Operating System. Many popular third-party programs utilize this interface including web browsers such as Mozilla Firefox and Google Chrome.

This vulnerability may be exploited if a user visits or is redirected to a specifically crafted web page. 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.

SYSTEMS AFFECTED:

- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft SQL Server 2000
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft BizTalk Server 2002
- Microsoft Commerce Server 2002

- Microsoft Commerce Server 2007
- Microsoft Commerce Server 2009
- Microsoft Visual FoxPro 8
- Microsoft Visual FoxPro 9
- Visual Basic 6.0 Runtime

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 has been discovered in Windows Common Controls that could allow an attacker to take complete control of a vulnerable system. Windows Common Controls are a set of ActiveX controls that enable a user to interact with an application. The vulnerable ActiveX control, MSCOMCTL.OCX, is included as part of all affected versions of the Microsoft software.

ActiveX controls are primarily used as building blocks for developing software components for use across multiple systems, usually over the Internet. The ActiveX controls are responsible for providing functionality across multiple interfaces and often enhance a user's experience.

The affected ActiveX Common Control, when used in Internet Explorer, corrupts the system state in such a way that an attacker can execute arbitrary code on the system. This vulnerability may be exploited if a user visits or is redirected to a specifically crafted web page. 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 the appropriate patch 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.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms12-027>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158>

SecurityFocus:

<http://www.securityfocus.com/bid/52911>