



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

February 9, 2010

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:

SA2010-008

SUBJECT:

Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (MS10-013)

OVERVIEW:

A vulnerability has been discovered in Microsoft DirectShow that could allow a remote attacker to take complete control of a vulnerable system. DirectShow is a component of Windows for streaming media and to perform various operations with media files on Microsoft Windows operating systems. This vulnerability can be exploited when a user opens a specially crafted media file. Successful exploitation could allow an attacker to gain 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 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

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 Microsoft DirectShow that could allow a remote attacker to take complete control of a vulnerable system. The vulnerability is caused by the DirectShow component improperly handling specially crafted Audio Video Interleave (AVI) files. This vulnerability can also be exploited when a user opens a specially crafted AVI file. AVI is a multimedia container format that is defined by Microsoft and is a common format for audio and video data on a computer. The specially crafted AVI file may be received via email or hosted on a web site.

Successful exploitation could allow an attacker to gain 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 download, accept, or execute media files from un-trusted or unknown 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.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/Ms10-013.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0250>