



**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:

SA2012-001

DATE(S) ISSUED:

01/10/2012

SUBJECT:

Vulnerabilities in Microsoft Windows Media Could Allow Remote Code Execution (MS12-004)

OVERVIEW:

Two vulnerabilities have been identified in Microsoft Media products. One has been identified in the Microsoft Windows Media Player application and another in Direct Show, both of which could allow remote code execution. Windows Media Player is a media library application that is used for playing audio, video, and viewing images. DirectShow is used for streaming media on Windows operating systems. It is a part of DirectX, which is a set of low level Application Programming Interfaces (APIs) used by Windows programs for multimedia support. Successful exploitation of this vulnerability 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:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows 7
- 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:

The first remote code execution vulnerability exists in the way that the Windows Media Player multimedia library (winmm.dll) handled a specially crafted MIDI file (.mid). The second remote code execution vulnerability is caused by the way that DirectShow filters do not properly handle specially crafted media files.

An attacker could take advantage of either of these issues by getting a user to open a specially crafted file via a website, email, or by hosting the file on a network share. Successful exploitation of either 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.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply the appropriate patch provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Do not 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/ms12-004>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0003>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0004>

Security Focus:

<http://www.securityfocus.com/bid/51292>

<http://www.securityfocus.com/bid/51295>