



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

December 13, 2011

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.

MS-ISAC ADVISORY NUMBER:

SA2011-066

DATE(S) ISSUED:

12/13/2011

SUBJECT:

Vulnerability in Windows Media Could Allow Remote Code Execution (MS11-092)

OVERVIEW:

A vulnerability has been identified in Microsoft Windows Media Center and Media Player applications that could allow remote code execution. Windows Media Center is a digital video recorder and media player. Windows Media Player is a media library application that is used for playing audio, video, and viewing images. 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 XP Media Center
- . Windows Vista
- . Windows 7

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 remote code execution vulnerability exists in the way that Windows Media Player and Windows Media Center parse specially crafted Microsoft Digital Video Recording (DVR-MS) media files. An attacker could take advantage of this issue 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 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.

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/ms11-092>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2011-3401>

Security Focus:

<http://www.securityfocus.com/bid/50957>