



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

March 8, 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.

ADVISORY NUMBER:

SA2011-013

DATE(S) ISSUED:

03/08/2011

SUBJECT:

Vulnerabilities in Windows Media Could Allow Remote Code Execution (MS11-015)

OVERVIEW:

Multiple vulnerabilities have been identified in Microsoft Windows Media technologies, specifically Windows Media Player, Windows Media Center, and DirectShow. Windows Media Player and Windows Media Center are digital media applications used for playing audio, video, and viewing images. DirectShow is a component of Windows for streaming media and to perform various operations with media files. Successful exploitation 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.

SYSTEMS AFFECTED:

- Windows XP
- Windows Media Center Edition 2005
- Windows Vista
- Windows Server 2008
- 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:**

Two remote code execution vulnerabilities have been discovered in Microsoft Windows Media technologies. Details of these vulnerabilities are as follows:

DirectShow Insecure Library Loading Vulnerability

This vulnerability exists due to the way .dll files are loaded by DirectShow. It allows an attacker to load a .dll of the attacker's choosing that could execute arbitrary code without the user's knowledge. The path of the attacker's .dll must be accessible via SMB/CIFS file share (UNC file paths, network or WebDAV shares) or local file system.

DVR-MS Vulnerability

This vulnerability exists due to the way .dvr-ms files are handled by 'SBE.dll'. The vulnerability can be exploited through a specially crafted .dvr-ms file or content that is hosted on a web page, delivered to the user via an e-mail, embedded in a Word document or any other multimedia file format.

Successful exploitation 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.

- Consider removing or restricting access to Windows Media Player in Windows installations if there is no business need for this software.
- Disable loading of libraries from WebDAV and remote network shares if there is no documented business need see Microsoft Knowledge Base Article 2264107 (<http://support.microsoft.com/kb/2264107>).

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms11-015.msp>
<http://support.microsoft.com/?kbid=810243>
[http://msdn.microsoft.com/en-us/library/ff919712\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ff919712(VS.85).aspx)
<http://www.microsoft.com/technet/security/advisory/2269637.msp>

Security Focus:

<http://www.securityfocus.com/bid/46680>

VUPEN:

<http://www.vupen.com/english/advisories/2011/0615>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2011-0032>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2011-0042>