

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.*

**DATE(S) ISSUED:**

8/11/2010

**SUBJECT:**

Vulnerability in Cinepak Codec Could Allow Remote Code Execution (MS10-055)

**OVERVIEW:**

A vulnerability has been discovered in the Cinepak Codec, which is used to compress and decompress digital media files. Cinepak is the primary video codec application for Microsoft Video for Windows and is used to compress and decompress digital media files on your computer. This vulnerability could allow remote code execution if a user opens a specially crafted media file (e.g. an AVI file). This vulnerability can be exploited via an email attachment or through the Web. Successful exploitation of this vulnerability 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:**

Windows XP SP 3  
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 vulnerability has been identified in the Cinepak Codec which could allow an attacker to take complete control of an affected system. Cinepak is the primary video codec application for Microsoft Video for Windows and is used to compress and decompress digital media files on your computer. This vulnerability is caused by a flaw within the iccvid.dll when handling a malformed VIDC compressed stream within an AVI file. This vulnerability can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted media file as an email attachment. In the Web based scenario, a user would have to open a specially crafted media file that is hosted on a website.

Successful exploitation of this vulnerability 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:**

The following actions should be taken:

- Apply appropriate patches 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 attachments and hypertext links contained in emails especially from un-trusted sources.

#### **REFERENCES:**

##### **Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/MS10-055.msp>

##### **Security Focus:**

<http://www.securityfocus.com/bid/42256>

##### **Secunia:**

<http://secunia.com/advisories/40936/>

##### **Tipping Point:**

<http://www.zerodayinitiative.com/advisories/ZDI-10-148/>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2553>