

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:

9/14/2010

SUBJECT:

Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution (MS10-062)

OVERVIEW:

A vulnerability has been discovered in the Microsoft MPEG-4 Codec that could allow an attacker to take complete control of a vulnerable system. A codec is software that is used to compress or decompress digital media content, such as a song or video. This vulnerability may be exploited if a user opens a specially crafted file, or visits or is redirected to a specifically crafted web page. Successful exploitation 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. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

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

A vulnerability has been discovered in the Microsoft MPEG-4 Codec which could allow an attacker to take complete control of an affected system. MPEG-4 is an International Standards Organization (ISO) specification that covers many aspects of multimedia presentation, including compression, authoring and delivery. The MPEG-4 codec used for MPEG-4 video decoding contains the vulnerable code.

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 visit or be redirected to a specially crafted website. Successful exploitation 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. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from 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/ms10-062.msp>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0818>