

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:

02/12/2013

SUBJECT:

Vulnerability in Media Decompression Could Allow Remote Code Execution (MS13-011)

OVERVIEW:

A remote code execution vulnerability exists in the way that Microsoft DirectShow handles media content. DirectShow is a media streaming architecture for Windows that allows video playback or capture. The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office document (such as a .ppt file) that contains a specially crafted embedded media file, or by visiting a website hosting specially crafted streaming content designed to exploit this vulnerability. This security update addresses the vulnerability by correcting the way that DirectShow handles specially crafted media content.

Successful exploitation 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 Service Pack 3
- Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Systems Service Pack 2

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 Microsoft Windows handles media content. The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office document (such as a .ppt file) that contains a specially crafted embedded media file, or by visiting a website hosting specially crafted streaming content designed to exploit this vulnerability.

Windows systems which use any of the following components are at risk from this vulnerability:

- Quartz.dll (DirectShow) on Windows XP Service Pack 3
- Quartz.dll (DirectShow) on Windows XP Professional x64 Edition Service Pack 2
- Quartz.dll (DirectShow) on Windows Server 2003 Service Pack 2
- Quartz.dll (DirectShow) on Windows Server 2003 x64 Edition Service Pack 2
- Quartz.dll (DirectShow) on Windows Server 2003 with SP2 for Itanium-based Systems
- Quartz.dll (DirectShow) on Windows Vista Service Pack 2
- Quartz.dll (DirectShow) on Windows Vista x64 Edition Service Pack 2
- Quartz.dll (DirectShow) on Windows Server 2008 for 32-bit Systems Service Pack 2
- Quartz.dll (DirectShow) on Windows Server 2008 for x64-based Systems Service Pack 2
- Quartz.dll (DirectShow) on Windows Server 2008 for Itanium-based Systems Service Pack 2

Successful exploitation 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.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

Remind users not to download or open files from un-trusted websites.

Remind users not to open email attachments from unknown or un-trusted sources.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms13-011>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2013-0077>