

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

June 8, 2010

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:

SA2010-038

DATE(S) ISSUED:

6/8/2010

SUBJECT:

Vulnerabilities in Media Decompression Could Allow Remote Code Execution (MS10-033)

OVERVIEW:

Two vulnerabilities have been discovered in Microsoft Windows that could allow a remote attacker to take complete control of an affected system. The vulnerabilities exist in the way Microsoft Windows handles media files. Exploitation can occur if a user visits a malicious web page or opens a malicious media file. 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 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

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 vulnerabilities have been discovered in Microsoft Windows that could allow a remote attacker to take complete control of an affected system. Exploitation can occur when Windows processes a media file with specially crafted compression data. Windows systems which use any of the following components are at risk from this vulnerability:

- DirectShow - DirectShow is a component of Windows for streaming media and to perform various operations with media files on Microsoft Windows operating systems.
- DirectX – DirectX is a collection of application programming interfaces for handling tasks related to multimedia on Microsoft platforms.
- Windows Media Format Runtime - Windows Media Format Runtime provides information to applications, such as Windows Media Player.
- Windows Media Encoder - Windows Media Encoder enables developers to convert or capture multimedia content for on-demand delivery (streaming).

Any Windows systems running client applications which use either the 'Asycfilt.dll' or 'Quartz.dll' libraries are vulnerable. Systems where MJPEG files are frequently processed are also at risk of being exploited.

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:

We recommend the following actions 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://www.microsoft.com/technet/security/bulletin/ms10-033.msp>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-1879>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-1880>

Security Focus:

<http://www.securityfocus.com/bid/40432>

<http://www.securityfocus.com/bid/40464>