

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

April 13, 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:

SA2010-028

DATE(S) ISSUED:

4/13/2010

SUBJECT:

Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (MS10-026)

OVERVIEW:

A vulnerability has been discovered in Microsoft MPEG Layer-3 codecs that could allow an attacker to take complete control of a vulnerable system. A codec is software that is used to compress or decompress a digital media file, such as a song or video. This vulnerability may be exploited if a user visits or is redirected to a specifically crafted web page, or opens a specially crafted file. 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 2000
- Windows XP
- 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 three Microsoft MPEG Layer-3 codecs which could allow an attacker to take complete control of an affected system. The three codecs that are vulnerable include the MPEG Layer-3 Audio Codec for Microsoft DirectShow (l3codecx.ax) and two Fraunhofer IIS MPEG Layer-3 ACM codecs (L3codeca.acm and L3codecp.acm). Specifically, this issue arises because the Microsoft MPEG Layer-3 codec does not perform sufficient boundary checks when processing a malicious Audio Video Interleave (AVI) file containing an MPEG Layer-3 audio stream. AVI is a multimedia container format that is defined by Microsoft and is a common format for audio and video data on a computer. The specially crafted AVI file may be received as an attachment via email or hosted on a web site.

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:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to download, accept, or execute media files from un-trusted or unknown sources.
- Remind users not to 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.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/Ms10-026.mspx>

<http://blogs.technet.com/srd/>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0480>

Secunia:

<http://secunia.com/advisories/39379>