



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

December 30, 2008

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.

DATE(S) ISSUED:

12/30/2008

SUBJECT:

Microsoft Windows Media Player WAV/MID/MIDI/SND File Parsing Integer Overflow Vulnerability

ORIGINAL OVERVIEW:

A vulnerability has been identified in Microsoft Windows Media Player. Windows Media Player is a digital media player and media library application that is used for playing audio, video, and viewing images. **This application is installed by default on all versions of Windows and is often set as the default media player.** Exploitation can occur if a user visits a specially crafted webpage or opens a malicious media file which takes advantage of this vulnerability. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. The attacker could then potentially access sensitive or confidential information, install programs, view, change, or delete data, or create new accounts.

At this time there is no patch and there are no workarounds available. Exploit code is available to the public.

UPDATED OVERVIEW:

Microsoft has reported that this vulnerability can not lead to remote code execution. Therefore, we have updated our risk analysis of this issue from High to Low for all entities.

SYSTEMS AFFECTED:

- Microsoft Windows Media Player 9
- Microsoft Windows Media Player 10
- Microsoft Windows Media Player 11

ORIGINAL 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

UPDATED RISK:

Government:

- **Large and medium government entities: Low**
- **Small government entities: Low**

Businesses:

- **Large and medium business entities: Low**
- **Small business entities: Low**

Home users: Low

ORIGINAL DESCRIPTION:

An integer overflow vulnerability has been discovered in the way versions of Microsoft Windows Media player handles specially crafted WAV, MID, and SND files. **Windows media player is often set as the default media player and can be executed by visiting a web page, opening an email attachment or opening a media file of the type WAV, MID, MIDI, or SND.** Successful exploitation will result in an attacker gaining the same privileges as the Windows Media Player process. The attacker could then potentially access sensitive or confidential information, install programs, view, change, or delete data, or create new accounts.

Proof of concept code for this vulnerability has been publicly released and verified in our lab to cause a denial of service condition. At this time we have not seen any reports of this vulnerability being exploited on the Internet.

At this time there is no patch and there are no workarounds available. Exploit code is available to the public.

UPDATED DESCRIPTION:

Microsoft has reported that this vulnerability can not lead to remote code execution. The proof of concept code will crash Windows Media but will not affect any other part of the system. This issue has been deemed a reliability issue by Microsoft.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- Do not accept or execute WAV, MID, MIDI, or SND files from untrusted or unknown sources.
- Do not download or open WAV, MID, MIDI, or SND files from un-trusted websites.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.

ORIGINAL REFERENCES:

SecurityFocus:

<http://www.securityfocus.com/bid/33018>

Cisco:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=17338>

Security Tracker:

<http://securitytracker.com/alerts/2008/Dec/1021495.html>

SANS Internet Storm Center:

<http://isc.sans.org/diary.html?storyid=5563>

UPDATED REFERENCES:

Microsoft:

<http://blogs.technet.com/msrc/archive/2008/12/29/questions-about-vulnerability-claim-in-windows-media-player.aspx>

<http://blogs.technet.com/swi/archive/2008/12/29/windows-media-player-crash-not-exploitable-for-code-execution.aspx>

SecurityFocus:

<http://www.securityfocus.com/bid/33018> - *BID has been RETIRED*

Security Tracker:

<http://securitytracker.com/alerts/2008/Dec/1021495.html>

ZDNET.com:

<http://blogs.zdnet.com/security/?p=2336>