CERT Advisory CA-2003-18 Integer Overflows in Microsoft Windows DirectX MIDI Library

Original issue date: July 25, 2003
Last revised: July 30, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Microsoft Windows systems running DirectX (Windows 98, 98SE, NT 4.0, NT 4.0 TSE, 2000, XP, Server 2003)

Overview

A set of integer overflows exists in a DirectX library included in Microsoft Windows. An attacker could exploit these vulnerabilities to execute arbitrary code or to cause a denial of service.

I. Description

Microsoft Windows operating systems include multimedia technologies called DirectX and DirectShow. From Microsoft Security Bulletin MS03-030, "DirectX consists of a set of low-level Application Programming Interfaces (APIs) that are used by Windows programs for multimedia support. Within DirectX, the DirectShow technology performs client-side audio and video sourcing, manipulation, and rendering."

DirectShow support for MIDI files is implemented in a library called quartz.dll. This library contains two vulnerabilities:

> *VU#561284 - Microsoft Windows DirectX MIDI library does not adequately validate Text or Copyright parameters in MIDI files*
>
> *VU#265232 - Microsoft Windows DirectX MIDI library does not adequately validate MThd track values in MIDI files*

In both cases, a specially crafted MIDI file could cause an integer overflow, leading to incorrect memory allocation and heap corruption.

Any application that uses DirectX/DirectShow to process MIDI files may be affected by these vulnerabilities. Of particular concern, Internet Explorer (IE) uses the Windows Media Player ActiveX control and quartz.dll to handle MIDI files embedded in HTML documents. An attacker could therefore exploit these vulnerabilities by convincing a victim to view an HTML document, such as a web page or an HTML email message, that contains an embedded MIDI file. Note that in addition to IE, a number of applications, including Outlook, Outlook Express, Eudora, AOL, Lotus Notes, and Adobe PhotoDeluxe, use the WebBrowser ActiveX control to interpret HTML documents.

Further technical details are available in eEye Digital Security advisory AD20030723. Common Vulnerabilities and Exposures (CVE) refers to these vulnerabilities as CAN-2003-0346.

II. Impact

By convincing a victim to access a specially crafted MIDI or HTML file, an attacker could execute arbitrary code with the privileges of the victim. The attacker could also cause a denial of service in any application that uses the vulnerable functions in quartz.dll.

III. Solution

Apply a patch

Apply the appropriate patch as specified by Microsoft Security Bulletin MS03-030.

The patch is a complete solution that fixes the integer overflows in quartz.dll. Sites that are unable to install the patch may consider the workaround described below.

Modify Internet Explorer settings

It is possible to significantly limit the ability of IE to automatically load MIDI files from HTML documents by making all of the following modifications:

- Disable *Active scripting*
- Disable *Run ActiveX controls and plug-ins*
- Disable *Play sounds in web pages*
- Disable *Play videos in web pages*

As stated above, the only complete solution for these vulnerabilities is to apply the patch. For example, Outlook Express 6 SP1 will play a MIDI file in an HTML email message regardless of the settings for audio and video in web pages. There may be other methods to automatically load a MIDI file from an HTML document. Also, these modifications will prevent some web pages from functioning properly.

Appendix A. Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft

> *Please see Microsoft Security Bulletin MS03-030.*

Appendix B. References

- CERT/CC Vulnerability Note VU#561284 - http://www.kb.cert.org/vuls/id/561284
- CERT/CC Vulnerability Note VU#265232 - http://www.kb.cert.org/vuls/id/265232
- eEye Digital Security advisory AD20030723 - http://www.eeye.com/html/Research/Advisories/AD20030723.html
- Microsoft Security Bulletin MS03-030 - http://microsoft.com/technet/security/bulletin/MS03-030.asp
- Microsoft Knowledge Base article 819696 - http://support.microsoft.com/default.aspx?scid=kb;en-us;819696

These vulnerabilities were researched and reported by eEye Digital Security. Jeff Johnson helped research the IE settings workaround.

Feedback can be directed to the author, Art Manion.

Revision History

July 25, 2003: Initial release, added Windows XP to Systems Affected
July 29, 2003: Removed IE security settings workaround from Solution
July 30, 2003: Updated IE settings workaround in Solution, changed references to vulnerabilities (plural), updated credits