

[NEWS] Unchecked Buffer in DirectX Could Enable System Compromise

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0103.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/24/03

To: list@securiteam.com

Date: 24 Jul 2003 16:30:27 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Unchecked Buffer in DirectX Could Enable System Compromise

SUMMARY

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.

There are two buffer overruns with identical effects in the function used by DirectShow to check parameters in a Musical Instrument Digital Interface (MIDI) file.

A security vulnerability results because it could be possible for a malicious user to attempt to exploit these flaws and execute code in the security context of the logged-on user.

An attacker could seek to exploit this vulnerability by creating a specially crafted MIDI file designed to exploit this vulnerability and then host it on a Web site or on a network share, or send it by using an HTML-based e-mail. In the case where the file was hosted on a Web site or

Securiteam: [NEWS] Unchecked Buffer in DirectX Could Enable System Compromise

network share, the user would need to open the specially crafted file. If the file was embedded in a page the vulnerability could be exploited when a user visited the Web page. In the HTML-based e-mail case, the vulnerability could be exploited when a user opened or previewed the HTML-based e-mail. A successful attack could cause DirectShow, or an application making use of DirectShow, to fail. A successful attack could also cause an attacker's code to run on the user's computer in the security context of the user.

DETAILS

Vulnerable Systems:

- * Microsoft DirectX® 5.2 on Windows 98
- * Microsoft DirectX 6.1 on Windows 98 SE
- * Microsoft DirectX 7.0a on Windows Millennium Edition
- * Microsoft DirectX 7.0 on Windows 2000
- * Microsoft DirectX 8.1 on Windows XP
- * Microsoft DirectX 8.1 on Windows Server 2003
- * Microsoft DirectX 9.0a when installed on Windows Millennium Edition
- * Microsoft DirectX 9.0a when installed on Windows 2000
- * Microsoft DirectX 9.0a when installed on Windows XP
- * Microsoft DirectX 9.0a when installed on Windows Server 2003
- * Microsoft Windows NT 4.0 with either Windows Media Player 6.4 or Internet Explorer 6 Service Pack 1 installed.
- * Microsoft Windows NT 4.0, Terminal Server Edition with either Windows Media Player 6.4 or Internet Explorer 6 Service Pack 1 installed.

Mitigating factors:

- * By default, Internet Explorer on Windows Server 2003 runs in [Enhanced Security Configuration](http://www.microsoft.com/downloads/details.aspx?FamilyID=d41b036c-e2e1-4960-99bb-9757f7e9e31b&Display=Enhanced%20Security%20Configuration). This default configuration of Internet Explorer blocks the e-mail-based vector of this attack because Microsoft Outlook Express running on Windows Server 2003 by default reads e-mail in plain text. If Internet Explorer Enhanced Security Configuration were disabled, the protections put in place that prevent this vulnerability from being exploited would be removed.
- * In the Web-based attack scenario, the attacker would have to host a Web site that contained a Web page used to exploit these vulnerabilities. An attacker would have no way to force users to visit a malicious Web site outside the HTML-based e-mail vector. Instead, the attacker would need to lure them there, typically by getting them to click a link that would take them to the attacker's site.
- * The combination of the above means that on Windows Server 2003 an administrator browsing only to trusted sites should be safe from this vulnerability.
- * Code executed on the system would only run under the privileges of the logged-on user.

Vulnerability identifier: CAN-2003-0346

What's the scope of this vulnerability?

This is a buffer overrun vulnerability. An attacker who successfully

Securiteam: [NEWS] Unchecked Buffer in DirectX Could Enable System Compromise

exploited the vulnerability could, in the worst case, run code of his or her choice on a user's system.

The attacker's code would run with the same privileges as the user: any restrictions on the user's ability to change the system would apply to the attacker's code.

For example, if the user were prevented from deleting files on the hard disk, the attacker's code would similarly be prevented.

Conversely, if a user were using an account with high privileges, such as an administrator's account, the attacker's code would also run with the same high privileges.

The vulnerability exists in the component responsible for parsing MIDI files. This function is included in a component of DirectX known as DirectShow.

What is DirectX?

Microsoft DirectX is a software component that contains a set of APIs that provide access to graphics acceleration chips and sound cards and other types of media hardware.

These APIs control low-level functions including: graphics acceleration, support for input devices (such as joysticks, keyboards, and mice) and control of sound mixing and sound output.

One of the technologies included in DirectX is called DirectShow.

What is DirectShow?

The DirectShow technology included in DirectX performs client-side audio and video sourcing, manipulation and rendering.

It supports several common media formats in addition to the affected MIDI file type, including Advanced Systems Format (ASF),

Motion Picture Experts Group (MPEG), Audio-Video Interleaved (AVI), MPEG Audio Layer-3 (MP3), and WAV sound files.

What are MIDI files?

A MIDI file is a special type of media file that outlines how the music is produced (for example, on a digital synthesizer) instead of representing the musical sound directly as other media files do.

This makes MIDI files much smaller than other audio files.

Are other media file formats affected by this vulnerability?

No. The vulnerability can only result when parsing specially crafted MIDI files. Other media files such as MPEG, MP3, WMV and AVI files are unaffected by this vulnerability.

What's wrong with DirectShow?

There are two buffer overruns with identical effects in the function used by DirectShow to check parameters in a MIDI (.MID) file.

A security vulnerability results because it is possible for a malicious user to attempt to exploit this flaw to execute code in the security context of the logged-on user.

If MIDI files are used by Windows Media and other technologies, does that mean there is a problem with Windows Media Player?

Securiteam: [NEWS] Unchecked Buffer in DirectX Could Enable System Compromise

No – The flaw is not in Windows Media Player. The flaw exists in DirectShow, and the way it checks the parameters of MIDI files. However, in the case of Windows NT 4.0, this technology was shipped in either Windows Media Player 6.4 or Internet Explorer 6 Service Pack 1.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by creating a specially crafted MIDI file and then taking one of several actions with it:

- * Host the file on a Web site or network share. In this case, if a user were to click the link or file, the vulnerability could be exploited.
- * If a user were to visit a Web site that had an embedded MIDI file, this could cause the vulnerability to be exploited.
- * Create an HTML-based e-mail message with a link to a Web page or a share that contained the file. If the user viewed the message in the preview pane or opened the message, the vulnerability could be exploited. In addition, an attacker could create an e-mail message with a link to a Web page or a share that contained the file, along with a suggestion that the user click the link.
- * Finally, an attacker could send a malformed MIDI file by using e-mail. An attacker could attach the file to an e-mail message and send it to a user with a suggestion that the user save the file on their system and then play it.

What could this vulnerability enable an attacker to do?

Successfully exploiting this vulnerability could, in the worst case, enable an attacker to run code of his or her choice on the user's system. Because DirectX runs in the context of the user, the attacker's code would also run as the user.

Any limitations on the user's ability to delete, add, or modify data or configuration information would also be applied to the attacker's code.

Why is Windows NT 4.0 vulnerable only when either Windows Media Player 6.4 or Internet Explorer 6 Service Pack 1 have been installed?

The file that contains the vulnerability is not installed, by default, on Windows NT 4.0. However, this file is installed when either Windows Media Player 6.4 or Internet Explorer 6 Service Pack 1 are installed on Windows NT 4.0.

I am running Internet Explorer on Windows Server 2003. Does this mitigate this vulnerability?

Yes. By default, Internet Explorer on Windows Server 2003 runs in a restricted mode known as Enhanced Security Configuration.

In this configuration, Internet Explorer prevents the automatic exploitation of this vulnerability through Outlook Express without user interaction.

This is done by setting Outlook Express to read e-mail as plain text as the default.

What is Internet Explorer Enhanced Security Configuration?

Internet Explorer Enhanced Security Configuration is a group of

Securiteam: [NEWS] Unchecked Buffer in DirectX Could Enable System Compromise

preconfigured Internet Explorer settings that reduce the likelihood of a user or administrator downloading and running malicious Web content on a server.

Internet Explorer Enhanced Security Configuration reduces this risk by modifying numerous security-related settings, including Security tab and Advanced tab settings in the Internet Options dialog box.

Disabling Internet Explorer Enhanced Security Configuration would remove the protections put in place that prevent these vulnerabilities from being exploited.

For more information regarding Internet Explorer Enhanced Security Configuration, please consult the Managing Internet Explorer Enhanced Security Configuration guide, which can be found at the following location:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=d41b036c-e2e1-4960-99bb-9757f7e9e31b&DisplayL>
<http://www.microsoft.com/downloads/details.aspx?FamilyID=d41b036c-e2e1-4960-99bb-9757f7e9e31b&DisplayL>

Is there any configuration of Windows Server 2003 that is likely to have Internet Explorer Enhanced Security Configuration disabled?

Yes. Systems administrators who have deployed Windows Server 2003 as a Terminal Server would likely disable Internet Explorer Enhanced Security Configuration to allow users of the Terminal Server to use Internet Explorer in an unrestricted mode.

How do I know which version of DirectX I have installed?

To check which version of DirectX that is installed on your system you need to run the DxDiag.exe command-line utility.

1. On the taskbar at the bottom of your screen, click Start, and then click Run.
2. In the Run dialog box, type dxdiag
3. Click OK.
4. On the System tab of the dialog box that appears, under System Information, the version of DirectX appears.

What does the patch do?

The patch eliminates the vulnerability by ensuring that DirectX correctly validates parameters when opening a MIDI file.

Patch availability

* Microsoft DirectX 5.2, DirectX 6.1 and DirectX 7.0a on

<http://microsoft.com/downloads/details.aspx?FamilyId=141D5F9E-07C1-462A-BAEF-5EAB5C851CF5&displayl>

Windows 98, Windows 98 SE and Windows Millennium Edition

Note: Windows 98, Windows 98 SE and Windows Millennium Edition users who are running a version of DirectX earlier than DirectX 9.0a must upgrade to DirectX 9.0b.

* Microsoft DirectX 7.0 on

<http://microsoft.com/downloads/details.aspx?FamilyId=7D0E4787-A993-4C49-A5A7-9A6DE8EFDB9E&displayl>

Windows 2000

* Microsoft DirectX 8.1 on

<http://microsoft.com/downloads/details.aspx?FamilyId=5ABA6A3B-F67B-4B18-B4B5-62E69A0104CE&displayl>

Securiteam: [NEWS] Unchecked Buffer in DirectX Could Enable System Compromise

Windows XP 32-bit Edition

* Microsoft DirectX 8.1 on

<<http://microsoft.com/downloads/details.aspx?FamilyId=8F23F7AF-5317-4502-8B17-7C1A2139EBDC&displaylan>

Windows XP 64-bit Edition

* Microsoft DirectX 8.1 on

<<http://microsoft.com/downloads/details.aspx?FamilyId=A5156FF8-1812-4DB4-9175-BF9CA370279D&displaylan>

Windows Server 2003 32-bit Edition

* Microsoft DirectX 8.1 on

<<http://microsoft.com/downloads/details.aspx?FamilyId=59732FCF-993A-45E8-8BA4-064575055D86&displaylan>

Windows Server 2003 64-bit Edition

* Microsoft DirectX 9.0a:

<<http://microsoft.com/downloads/details.aspx?FamilyId=22F990CB-E9F9-4670-8B4F-AC4F6F66C3A2&displaylan>

All Windows versions

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=B42C5BCB-6D36-437D-A07E-053B72B1C652&displaylan>

Microsoft Windows NT 4.0

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=14290AD7-EE7D-4736-8322-BCA4CBD7D7C5&displaylan>

Microsoft Windows NT 4.0, Terminal Server Edition

Note: DirectX 9.0b has been released at the same time as this security bulletin and contains the security fix discussed in the security bulletin. DirectX 9.0b can be installed on all versions of Windows except Windows NT 4.0 and can be downloaded from the following location:

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=141D5F9E-07C1-462A-BAEF-5EAB5C851CF5&displaylan>

All Windows Versions except Windows NT 4.0

ADDITIONAL INFORMATION

Vulnerability discovered by <<http://www.eeye.com>> eEye Digital Security

Original article can be found at:

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-030.asp?frame=true&hi>
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-030.asp?frame=true&hid>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.