

[NT] Flaw In Windows Media Player May Allow Media Library Access

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0095.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/25/03

To: list@securiteam.com

Date: 25 Jun 2003 22:19:13 +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

Flaw In Windows Media Player May Allow Media Library Access

SUMMARY

An ActiveX control included with Windows Media Player 9 Series allows Web page authors to create Web pages that can play media and provide a user interface by which the user can control playback. When a user visits a Web page with embedded media, the ActiveX control provides a user interface that allows the user to take such actions as pausing or rewinding the media.

A flaw exists in the way in which the ActiveX control provides access to information on the user's computer. A vulnerability exists because an attacker could invoke the ActiveX control from script code, which would allow the attacker to view and manipulate metadata contained in the media library on the user's computer.

To exploit this flaw, an attacker would have to host a malicious Web site that contained a Web page designed to exploit this vulnerability, and then persuade a user to visit that site – an attacker would have no way to

Securiteam: [NT] Flaw In Windows Media Player May Allow Media Library Access

force a user to the site. An attacker could also embed a link to the malicious site in an HTML e-mail and send it to the user. After the user previewed or opened the e-mail, the malicious site could be visited automatically without further user interaction.

The attacker would only have access to manipulate the media library on the user's computer. The attacker would not be able to browse the user's hard disk and would not have access to passwords or encrypted data. The attacker would not be able to modify files on the user's hard disk, but could modify the contents of any Media Library entries associated with those files. The attacker might also be able to determine the user name of the logged-on user by examining the directory paths to media files.

DETAILS

Affected Software:

- * Microsoft Windows Media Player 9 Series

Not Affected Software Versions:

- * Microsoft Windows Media Player 6.4
- * Microsoft Windows Media Player 7.1
- * Microsoft Windows Media Player for Windows XP (8.0)

Mitigating factors:

- * By default, Internet Explorer on Windows Server 2003 runs in Enhanced Security Configuration. This default configuration of Internet Explorer blocks this attack.
- * The attacker could only gain access to information contained in the Windows Media Library
- * The attacker would not be able to execute code on the system or delete files on the user's hard disk.

Patch availability:

Download locations for this patch

The patch to correct this vulnerability can be downloaded from the following locations:

–

<http://microsoft.com/downloads/details.aspx?FamilyId=36814221-8194-4492-BB29-94DB3D4CB682&displaylan>
Windows Media Player 9 Series

–

<http://microsoft.com/downloads/details.aspx?FamilyId=82CD6192-15D8-4E28-9B14-F9B78FF01D8A&displaylan>
Windows Media Player 9 Series on Windows Server 2003

What's the scope of the vulnerability?

This is an information disclosure vulnerability. An attacker who successfully exploited this vulnerability could gain access to a user's media library without the user being aware of this access.

Does this vulnerability affect all versions of Windows Media Player?

No – only Windows Media Player 9 Series is affected.

Securiteam: [NT] Flaw In Windows Media Player May Allow Media Library Access

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by hosting a specially constructed Web page. If a user were to visit this Web page, the Windows Media Player 9 Series ActiveX control would load and the attacker could then use script code to invoke the control and cause it to provide the attacker with access to the user's media library. As an alternative, an attacker could craft an HTML e-mail that attempted to exploit this vulnerability.

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to view and manipulate information in the user's media library. This vulnerability could allow an attacker to change the metadata of media files, delete entries from the media library, or rename entries in the library. The attacker could not delete or rename the actual media files on the user's hard disk; he or she could only manipulate entries in the library. However the attacker might be able to determine the user name of the logged in user by examining the directory paths to the media files.

What is Media Library Metadata?

Windows Media Player Library entries contain information about media files. This information is called metadata. Metadata is information about a song or video file such as artist name, track name, album name, or genre. This information, which is often provided automatically when a user records music from CDs into digital music, is stored in the media library of Windows Media Player.

What causes the vulnerability?

The vulnerability results because the Windows Media Player 9 Series ActiveX control does not properly validate access to the Media Library.

What's wrong with the way Windows Media Player 9 Series provides access to the Media Library?

The Windows Media Player 9 Series ActiveX control uses the Windows Media Player public object model, and provides access to the media library under certain conditions. The Windows Media Player 9 Series ActiveX control is a scriptable component, meaning that script code can be used to invoke or control it. The ActiveX control does not properly validate requests made by script to access the Media Library.

What are ActiveX controls?

ActiveX is a technology that allows Web authors the ability to embed small programs in Web pages or other interfaces to provide additional functionality. These embedded programs are known as ActiveX Controls. Developers can create ActiveX controls in any programming language that supports the Microsoft Common Object Model.

I have my Windows Media Player 9 Series configured to not run script automatically. Does this protect me from this vulnerability?

No – in this case it is the ActiveX control running the script code that allows access to the Media Library, not the Windows Media Player itself.

Securiteam: [NT] Flaw In Windows Media Player May Allow Media Library Access

The flaw exists because the ActiveX Control does not properly validate who is accessing the Media Library.

What products does Windows Media Player 9 Series ship with?

Windows Media Player 9 Series is included with Windows Server 2003. In addition it can be downloaded as an update for Windows XP, Windows 2000, Windows ME and Windows 98 Second Edition.

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

Yes. By default, Internet Explorer on Windows Server 2003 runs in a restricted mode known as Enhanced Security Configuration. In this configuration the ActiveX control would not load.

What is Internet Explorer Enhanced Security Configuration?

Internet Explorer Enhanced Security Configuration is a group of 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 threat by modifying numerous security-related settings, including Security and Advanced tab settings in Internet Options. Some of the key modifications include:

- * Security level for the Internet zone is set to High. This setting disables scripts, ActiveX components, Microsoft virtual machine (Microsoft VM) HTML content, and file downloads.

- * Automatic detection of intranet sites is disabled. This setting assigns all intranet Web sites and all Universal Naming Convention (UNC) paths that are not explicitly listed in the Local intranet zone to the Internet zone.

- * Install on Demand and non-Microsoft browser extensions are disabled. This setting prevents Web pages from automatically installing components and prevents non-Microsoft extensions from running.

- * Multimedia content is disabled. This setting prevents music, animations, and video clips from running.

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&Display=...>
<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 Servers would likely disable Internet Explorer Enhanced Security Configuration to allow users of the Terminal Server to utilize Internet Explorer in an unrestricted mode.

Securiteam: [NT] Flaw In Windows Media Player May Allow Media Library Access

What does the patch do?

The patch eliminates the vulnerability by ensuring the Windows Media Player 9 Series ActiveX Control properly validates access to the Media Library.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_49448_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>
Microsoft Product Security.

=====

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.