

[NT] Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0096.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/25/03

To: list@securiteam.com

Date: 25 Jun 2003 22:27:56 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.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 ISAPI Extension for Windows Media Services Could Cause Code Execution

SUMMARY

Microsoft Windows Media Services is a feature of Microsoft Windows 2000 Server, Advanced Server, and Datacenter Server and is also available in a downloadable version for Windows NT 4.0 Server. Windows Media Services contains support for a method of delivering media content to clients across a network known as multicast streaming. In multicast streaming, the server has no connection to or knowledge of the clients that may be receiving the stream of media content coming from the server. To facilitate logging of client information for the server, Windows 2000 includes a capability specifically designed to enable logging for multicast transmissions.

This logging capability is implemented as an Internet Services Application Programming Interface (ISAPI) extension – `nsiislog.dll`. When Windows Media Services are added through add/remove programs to Windows 2000, `nsiislog.dll` is installed in the Internet Information Services (IIS)

Securiteam: [NT] Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution

Scripts directory on the server. Once Windows Media Services is installed, nsiislog.dll is automatically loaded and used by IIS.

There is a flaw in the way nsiislog.dll processes incoming client requests. A vulnerability exists because an attacker could send specially formed HTTP request (communications) to the server that could cause IIS to fail or execute code on the user's system.

Windows Media Services is not installed by default on Windows 2000. An attacker attempting to exploit this vulnerability would have to be aware which computers on the network had Windows Media Services installed on it and send a specific request to that server.

DETAILS

Affected Software:

- * Microsoft Windows 2000

Not Affected Software Versions:

- * Windows NT 4.0
- * Microsoft Windows XP
- * Microsoft Windows Server 2003

Mitigating factors:

- * Windows Media Services 4.1 is not installed by default on Windows 2000.
- * Windows Media Services are not available for Windows 2000 Professional.

Patch availability:

Download locations for this patch

- * Microsoft Windows 2000:

<http://microsoft.com/downloads/details.aspx?FamilyId=F772E131-BBC9-4B34-9E78-F71D9742FED8&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=F772E131-BBC9-4B34-9E78-F71D9742FED8&displaylang=de>

What's the scope of the vulnerability?

This is a Buffer Overrun vulnerability. An attacker who successfully exploited this vulnerability could cause a Windows 2000 server that was performing streaming media logging to fail in a way that could allow code to execute in the security context of the IIS service.

How could an attacker exploit this vulnerability?

An attacker could exploit this vulnerability by constructing a specific network request and sending it to the server running Windows Media Services. The attacker would have to know which server on the network or Internet had Windows Media Services installed in order to cause the server to stop responding to IIS requests or cause code to execute in the server.

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to execute code of his or her choice on a computer running IIS with Windows Media Services installed.

Securiteam: [NT] Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution

The code would execute in the context of the account under which IIS was running, which could allow the attacker to take any action on the system.

What causes the vulnerability?

The vulnerability results because of an unchecked buffer used by nsiislog.dll, the streaming media component that is used to log multicast requests. If a specially crafted request was sent to the server, the logging program would attempt to write a larger buffer than was available, which then in turn could cause the IIS service to fail and could allow code of the attacker's choice to execute.

What is nsiislog.dll?

Nsiislog.dll is an IIS ISAPI extension that is included with Windows 2000 Server. It provides logging capabilities for Media Streaming in Microsoft Windows Media Services. It is installed and used automatically whenever Windows Media Services are installed on a computer.

What versions of IIS might be affected by the vulnerable version of nsiislog.dll?

The vulnerable version of nsiislog.dll can be installed on IIS 5.0.

What products does IIS 5.0 ship with?

Internet Information Service 5.0 is included with Windows 2000 Datacenter Server, Advanced Server, Server and Professional.

Does IIS 5.0 run by default?

IIS 5.0 runs by default on all Windows 2000 server products. It does not run by default on Windows 2000 Professional.

What are Microsoft Windows Media Services?

Windows Media Services is a feature of Windows 2000 Server, Advanced Server, and Datacenter Server and provides streaming audio and video services for use over corporate intranets and the Internet.

Can I install Windows Media Services on Windows 2000 Professional?

No – Windows Media Services are only available for Microsoft Windows Server operating systems, such as Windows 2000 Server, Advanced Server and Datacenter Server.

Does this vulnerability affect Windows Media Services on Windows NT 4.0?

That depends. If you have applied the previous patch for Windows Media Servers from security bulletin MS03–019, this vulnerability does not affect Windows NT 4.0.

What is Multicast Media Streaming?

Multicast media streaming is a method of delivering media content to clients across a network. In contrast to unicast media streaming, multicasting sends a single copy of the data that can be received by any clients that request it. Multiple copies of data are not sent across the network, nor is data processed by clients who do not request it. For more information on Multicast Media Streaming, please see the following web

Securiteam: [NT] Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution

site: <<http://www.microsoft.com/windows/windowsmedia/serve/multiwp.aspx>>
<http://www.microsoft.com/windows/windowsmedia/serve/multiwp.aspx>

How can I determine whether someone has set up my computer to perform multicast streaming media logging?

If you have installed Windows Media Services on Windows 2000 Server, then the nsiislog.dll file is automatically copied to the proper IIS directory and loaded. To determine if nsiislog.dll is installed on the computer, perform the following steps:

- * From the Start Menu, click search.
- * Click For Files or Folders
- * In the search dialog, type in the file name, NSIISLOG.DLL
- * Click Search Now.

If the file NSIISLOG.DLL is present in any directory shared by IIS, then the server is configured for logging clients of multicast streams.

What does the Patch do?

The fix eliminates the vulnerability by ensuring that the Nsiislog.dll file correctly responds to requests.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:0_49449_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.