

[NT] Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0063.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/29/03

To: list@securiteam.com

Date: 29 May 2003 23:27:22 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service

SUMMARY

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

This capability is implemented as an Internet Services Application Programming Interface (ISAPI) extension – `nsiislog.dll`. When Windows Media Services are installed in Windows NT 4.0 Server or added through add/remove programs to Windows 2000, `nsiislog.dll` is installed to the

Securiteam: [NT] Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service

Internet Information Services (IIS) Scripts directory on the server.

There is a flaw in the way in which nsiislog.dll processes incoming requests. A vulnerability exists because an attacker could send specially formed communications to the server that could cause IIS to stop responding to Internet requests.

Windows Media Services is not installed by default on Windows 2000, and must be downloaded to install on Windows NT 4.0. 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. The denial of service would only affect IIS, and other services on the server would remain unaffected.

DETAILS

Affected Software:

- * Microsoft Windows NT 4.0
- * Microsoft Windows 2000

Non Affected Software:

- * Microsoft Windows XP
- * Microsoft Windows Server 2003

Mitigating factors:

- * Windows Media Services 4.1 is not installed by default on Windows 2000, and must be downloaded to install on Windows NT 4.0.
- * Windows Media Services are not available for Windows 2000 Professional or Windows NT 4.0 Workstation
- * The attacker would have to know which server on the network Windows Media Services had been installed on.

Patch availability:

Download locations for this patch

- * Microsoft Windows NT 4.0:

<http://microsoft.com/downloads/details.aspx?FamilyId=8D7E3716-1AA7-4EDC-B084-7D50C8D3C2AB&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=8D7E3716-1AA7-4EDC-B084-7D50C8D3C2AB&displaylang=de>

- * Microsoft Windows 2000:

<http://microsoft.com/downloads/details.aspx?FamilyId=9EFA4EBD-2068-4742-917D-A2638688C029&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=9EFA4EBD-2068-4742-917D-A2638688C029&displaylang=de>

What's the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who successfully exploited this vulnerability could cause a Windows 2000 or Windows NT 4.0 server to stop responding to web page requests.

How can an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by constructing a

Securiteam: [NT] Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service

specific network request and sending it to the server performing logging. The attacker would have to know which server on the network or internet was performing logging in order to cause the server to stop responding to IIS requests.

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to cause a denial of service on a computer running IIS with streaming media logging enabled.

What causes the vulnerability?

The vulnerability results because of an unchecked buffer used by the nsiislog.dll file for logging. If a specially crafted request is sent to the server, the logging file will attempt to write a larger buffer than is possible, which then in turn causes the IIS service to fail.

What is nsiislog.dll?

Nsiislog.dll is an IIS ISAPI extension that was shipped as part of Windows 2000 Server and Advanced Server to provide logging capabilities for Media Streaming in Microsoft Media Services.

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

The vulnerable version of nsiislog.dll can be installed into IIS 4.0, and 5.0.

What products do IIS 4.0 and 5.0 ship with?

* Internet Information Server 4.0 ships as part of the Windows NT 4.0 Option Pack (NTOP).

* Internet Information Service 5.0 ships as part of Windows 2000 Datacenter Server, Advanced Server, Server and Professional.

Do IIS 4.0, and 5.0 run by default?

* IIS 4.0 runs by default when the NTOP is installed on a Windows NT 4.0 server. It does not run by default when the NTOP is installed on a Windows NT 4.0 workstation, unless Peer Web Services were already running when it was installed.

* 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 over corporate intranets and the Internet. In addition, a downloadable version can be added to Windows NT 4.0.

Can I install Windows Media Services into Windows 2000 Professional or Windows NT 4.0 Workstation?

No – Windows Media Services are only available for Microsoft Windows Server operating systems, such as Windows 2000 Server, Advanced Server and Datacenter Server, or Windows NT 4.0 Server.

Securiteam: [NT] Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service

What is Multicast Media Streaming?

Multicast media streaming is a method of delivering media content to clients across a network. As opposed to unicast, method of media streaming, multicasting sends a single copy of the data to those clients who request it. Multiple copies of data are not sent across the network, nor is data processed by clients who do not want it. For more information on Multicast Media Streaming, please see the following web site:
<<http://www.microsoft.com/windows/windowsmedia/serve/multiwp.aspx>>
<http://www.microsoft.com/windows/windowsmedia/serve/multiwp.aspx>

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

To determine if your computer has been configured for multicast streaming media logging, 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 NSISSLOG.DLL is present in any directory shared by IIS, then the server is configured for logging of clients of multicast streams.

What does the Patch do?

The fix eliminates the potential for a denial of service attack by ensuring that the Nsiislog.dll file correctly responds to requests.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:0_48426_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.