

Alert: Microsoft Security Bulletin – MS03–022

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-06/0045.html>

From: Russ (*Russ.Cooper_at_RC.ON.CA*)

Date: 06/25/03

Date: Wed, 25 Jun 2003 13:10:48 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

<http://www.microsoft.com/technet/security/bulletin/MS03-022.asp>

Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution (822343)

Originally posted: June 25, 2003

Summary

Who should read this bulletin: System administrators running Microsoft® Windows® 2000

Impact of vulnerability: Allow an attacker to execute code of their choice

Maximum Severity Rating: Important

Recommendation: System administrators should install the patch at the earliest available opportunity.

End User Bulletin: An end user version of this bulletin is available at:

http://www.microsoft.com/security/security_bulletins/ms03-022.asp.

Affected Software:

– Microsoft Windows 2000

Not Affected Software Versions:

– Windows NT 4.0

– Microsoft Windows XP

– Microsoft Windows Server 2003

Technical description:

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.

NT-Bugtraq: Alert: Microsoft Security Bulletin – MS03-022

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) 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.

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.

Vulnerability identifier: CAN-2003-0349

This email is sent to NTBugtraq automatically as a service to my subscribers. (v1.18)

Cheers,

Russ – Surgeon General of TruSecure Corporation/NTBugtraq Editor

oo

Are You "Certifiable"? Summer's Hottest Certification Just Got HOTTER!

With a growth rate exceeding 110%, the TICSAs security practitioner certification is one of the hottest IT credentials available. And now, for a limited time, you can save 33% off of the TICSAs certification exam! To learn more about the TICSAs certification, and to register as a TICSAs candidate online, just go to

<http://www.trusecure.com/offer/s0100/>

oo