

Re: NetMeeting on Internal LAN?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2001-07/0049.html>

From: J.D. Meek ([jdmeek at edgenet.com](mailto:jdmeek@edgenet.com))

Date: 07/18/01

Just verified this on Win98 w/ Netmeeting3.01 as well. Not to mention the fact that you don't have to be in a call for this to work. Simply having NM open is enough for this to work.

Nir Aran wrote:

> -----BEGIN PGP SIGNED MESSAGE-----
>
> Enjoy :-)
>
> =TAnin
>
> Diversified Software Industries, Inc.
> www.dsi-inc.net/dsi
> Security Advisory
>
> October 16, 2000
>
> Denial of Service attack against computers running Microsoft
> NetMeeting
>
> 1. Description
> 2. Steps to reproduce (exploit)
> 3. Vendor status and solution
> 4. Disclaimer
> 5. Credits
> 6. About DSI
>
> -----
> 1. Description
>
> NetMeeting is a free software product from Microsoft which allows
> realtime
> audio/video conferencing among peer computers. NetMeeting also
> contains a
> component known as Remote Desktop Sharing (RDS). RDS allows a
> technician to
> take remote control of computers for troubleshooting, etc. RDS has
> some uses
> which are similar to (but more limited than) Terminal Services,
> pcAnywhere,

SecurityFocus BASICS: Re: NetMeeting on Internal LAN?

> etc.
>
> *The exploit below has been tested against the current version of*
> *NetMeeting*
> *3.01 which ships with Windows 2000. It has been tested on Windows*
> *95, NT 4*
> *Workstation and Server SP5/6, and Windows 2000 Workstation and Server*
> *SP1.*
> *It has been tested against computers with either modem or ethernet*
> *connections.*
> -----
> *2. Steps to reproduce (exploit)*
>
> *In this example, my.unix.box.com represents the attacker, and*
> *hapless.victim.com represents the computer running NetMeeting in*
> *either*
> *client or RDS mode.*
>
> *Assuming you already have netcat installed on my.unix.box.com, enter*
> *the*
> *following command line:*
>
> *nc hapless.victim.com 1720 < /dev/zero*
>
> *At this point, CPU usage on the victim machine becomes elevated,*
> *depending*
> *on the speed of both machines, and the speed of the link between*
> *them.*
>
> *Now, terminate the netcat command with ^C. At this point, CPU on the*
> *victim*
> *machine hits 100% and stays there. If NetMeeting is running in*
> *client mode,*
> *it can (eventually) be terminated via the Task Manager on Windows*
> *2000 or*
> *NT. If RDS is active, it may be necessary to use another tool (such*
> *as*
> *HandleEx) to terminate the RDS service; Task Manager may not have*
> *access to*
> *this process.*
>
> *If you are using RDS for remote server management, you may now need*
> *to make*
> *a road trip to the remote computer to restore functionality.*
> -----
> *3. Vendor status and solution*
>
> *Microsoft has released a patch for Windows 2000. Microsoft's*
> *bulletin is*
> *available at*
> *<http://www.microsoft.com/technet/security/bulletin/MS00-077.asp>*

SecurityFocus BASICS: Re: NetMeeting on Internal LAN?

>
> *NOTE: At this time, there are some issues with the NT 4.0 patch
> installer.
> Microsoft is working to fix these issues, and an updated installer
> should be
> available when complete.*
> -----
> *4. Disclaimer*
>
> *The information in this advisory is believed to be accurate. No
> warranty is
> given, express or implied. Neither the author nor the publisher
> accepts any
> liability whatsoever for any use of this information, nor do we
> condone the
> use of this information for unethical purposes.*
> -----
> *5. Credits*
>
> *We would like to acknowledge Microsoft for their efforts to fix this
> problem. Also, we would like to acknowledge SecureXpert Labs for
> their
> advisory SX-20000620-2 (see also MS00-050) which pointed out other
> Microsoft
> services potentially vulnerable to /dev/zero attacks.*
> -----
> *6. About DSI*
>
> *Diversified Software Industries, Inc. is an Iowa City/Coralville,
> Iowa-based
> company that develops and markets software for the graphical
> representation
> of data in vehicles. In addition, DSI markets custom software
> development
> and project management skills to firms in the over-the-road
> transportation
> marketplace. These custom solutions provide back office and
> on-vehicle
> wireless messaging management, as well as dispatching and resource
> tracking
> systems.*
>
> *You can find more information about DSI at www.dsi-inc.net/dsi*
>
> -----Original Message-----
> *From: Stephen Zeigler [mailto:SZeigle_at_smud.org]
> Sent: Friday, July 13, 2001 5:46 PM
> To: 'SECURITY-BASICS_at_securityfocus.com'
> Subject: NetMeeting on Internal LAN?*
>
> *Hi all,*

Re: NetMeeting on Internal LAN?

SecurityFocus BASICS: Re: NetMeeting on Internal LAN?

> *Is anyone familiar with the risks associated with using NetMeeting on*
> *an*
> *internal LAN? One of our users wants to use it to share an*
> *application with*
> *others on our internal network. Collaboration mode would not be used*
> *and*
> *they would not automatically accept calls... I've done some cursory*
> *investigation and exposure seems to be using this product on the web.*
>
> *Stephen Zeigler*
> *Network Design & Development (Security)*
> *Work (916) 732.6952*
> *Cell (916) 826.6268*
> *Fax (916) 732.7521*
> *szeigle at smud.org*
> *MS C105*
>
> -----BEGIN PGP SIGNATURE-----
> Version: PGPfreeware 6.5.8 for non-commercial use <<http://www.pgp.com>>
>
> iQEVAwUBO0/yr+oRYpbiWTZdAQHWSgf/WrdaiETtdQ97pOKjkrQi1/VfnOa+9XJq
> d0DWK9AskThnyM05oKIqcbB6/ywrBT7qxFdr+uWZ2auHHWg7lAmcksW/zH+o58RK
> /rQNArjoP9rs1KLoZs7viuNdF/4OSivuGed1xMtW85Jv2sC9RddyFXbFJELOQvzz
> ZX9J71iWC7r5t+lA9T27/tGwmVCJPVeZc6NZLnGBMeCW9aa1srHvVGdISeeqyIJ
> vtAwZmepbPGwlInVdFFviJfZAnk0JRZtT1sq3vDGJOza+m/0FRWuIt3rF0frDcw7
> 30HsvDTK/aSiFUpJIwoysfln8Z4oCS3MTcYvEskeWjpBudgSb0GQ1Q==
> =XrYW
> -----END PGP SIGNATURE-----

- ***Vorherige Nachricht:*** Smith, Chris: "RE: Port scanning"
- ***Nachrichten sortiert nach:*** [Datum] [Thread] [Subject] [Autor] [Attachment]