

[NT] Vulnerability in NNTP Allows Remote Code Execution (MS04-036)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0051.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/13/04

To: list@securiteam.com

Date: 13 Oct 2004 18:32:15 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Vulnerability in NNTP Allows Remote Code Execution (MS04-036)

SUMMARY

A remote code execution vulnerability exists within the Network News Transfer Protocol (NNTP) component of the affected operating systems. This vulnerability could potentially affect systems that do not use NNTP. This is because some programs that are listed in the affected software section require that the NNTP component be enabled before you can install them.

DETAILS

Vulnerable Systems:

* Microsoft Windows NT Server 4.0 Service Pack 6a –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0126B7AC-9C78-45C5-8AC7-E0E8CA4B6DEE>>

Download the update

* Microsoft Windows 2000 Server Service Pack 3 and Microsoft Windows 2000 Server Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=54A86560-4A0C-4E2F-A137-D8EE905A674A>>

Download the update

* Microsoft Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=DCB1CB73-A426-40D8-BD14-B458C7915815>>

Download the update

Securiteam: [NT] Vulnerability in NNTP Allows Remote Code Execution (MS04-036)

* Microsoft Windows Server 2003 64-Bit Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1A8C4D7A-2F85-4CDD-8CC9-E2E1817403DF>>

Download the update

* Microsoft Exchange 2000 Server Service Pack 3 (Uses the Windows 2000 NNTP component)

* Microsoft Exchange Server 2003 and Microsoft Exchange Server 2003 Service Pack 1 (Uses the Windows 2000 or Windows Server 2003 NNTP component)

Immune Systems:

* Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

* Microsoft Windows 2000 Professional Service Pack 3 and Microsoft Windows 2000 Professional Service Pack 4

* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

* Microsoft Windows XP 64-Bit Edition Service Pack 1

* Microsoft Windows XP 64-Bit Edition Version 2003

* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

* Microsoft Exchange Server 5.0 Service Pack 2

* Microsoft Exchange Server 5.5 Service Pack 4

Affected Components:

* Microsoft Windows NT Server 4.0 Service Pack 6a NNTP component

* Microsoft Windows 2000 Server Service Pack 3 NNTP component and Microsoft Windows 2000 Server Service Pack 4 NNTP component

* Microsoft Windows Server 2003 NNTP Component

* Microsoft Windows Server 2003 64-Bit Edition NNTP Component

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0574>>

CAN-2004-0574

* Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed. If the affected NNTP Ports (119 and 563) are blocked at the firewall, external attacks attempting to exploit this vulnerability could be blocked.

* Windows NT Server 4.0, Windows 2000 Server, and Windows Server 2003 are at a reduced risk from this vulnerability because the affected component is not installed by default. Even if Internet Information Services is installed, the affected component is not installed by default. An administrator must manually install the affected component for a system to become vulnerable to this issue.

* Exchange 2000 Server and Exchange Server 2003 require the installation of the affected operating system component. However upon installation, Exchange Server 2003 disables the affected operating system component. Exchange Server 2003 requires an administrator to manually re-enable this

Securiteam: [NT] Vulnerability in NNTP Allows Remote Code Execution (MS04-036)

component to become vulnerable to this issue. Exchange 2000 Server does not disable this component by default when it is installed. However, if an administrator manually disables this component after installing Exchange Server 2000, the system is not vulnerable to this issue. Best practice recommendations for helping to secure Exchange 2000 Server include disabling the affected operating system component. For more information about how to help secure Exchange 2000 Server, visit the following <<http://www.microsoft.com/technet/security/guidance/secmod43.msp>> Web site.

Workarounds for NNTP Vulnerability

- * Block the following at the firewall:
 - * UDP ports 119 and 563
 - * TCP ports 119 and 563

These ports are used to initiate a connection with a NNTP server. Blocking them at the firewall will help prevent systems that are behind that firewall from attempts to exploit this vulnerability. Also, make sure that you block any other specifically configured NNTP ports on the system. We recommend that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about the ports that NNTP uses, visit the following <<http://go.microsoft.com/fwlink/?LinkId=21312>> Web site. Port 563 is the default port that NNTP uses to perform Secure Sockets Layer (SSL) connections.

- * Enable advanced TCP/IP filtering on systems that support this feature. You can enable advanced TCP/IP filtering to block the affected ports and to block all unsolicited inbound traffic. For more information about how to configure TCP/IP filtering, see Microsoft Knowledge Base Article <<http://support.microsoft.com/default.aspx?scid=kb:en-us:309798>> 309798.

- * Block the affected ports by using IPsec on the affected systems. Use Internet Protocol security (IPsec) to help protect network communications. Detailed information about IPsec and how to apply filters is available in Microsoft Knowledge Base Articles <<http://support.microsoft.com/default.aspx?scid=kb:en-us:313190>> 313190 and <<http://support.microsoft.com/?id=813878>> 813878.

- * Remove or disable NNTP if you do not need it: In many organizations, NNTP only provides services for legacy systems. If you no longer need NNTP, you could remove it by following these steps. These steps apply only to Windows 2000 and later versions. For Windows NT 4.0, follow the procedure that is included in the product documentation. NNTP is a required component for Exchange 2000 Server and Exchange Server 2003. However, while NNTP may not be removed on Exchange servers, it can be disabled. NNTP is disabled by default on Exchange 2003. To help secure Exchange 2000 systems, follow the <Securing Exchange 2000 Server> Securing Exchange 2000 Server best practice recommendations instead of these instructions.

Securiteam: [NT] Vulnerability in NNTP Allows Remote Code Execution (MS04-036)

How could an attacker exploit the vulnerability ?

An attacker could exploit the vulnerability by creating a specially crafted message and sending the message to an affected system, which could then cause the affected system to execute code.

An attacker could also access the affected component through another vector. For example, an attacker could log on to the system interactively or by using another program that passes parameters to the vulnerable component (locally or remotely).

What systems are primarily at risk from the vulnerability ?

Windows 2000 Professional (all versions), and Windows XP (all versions) are not affected by this vulnerability. The affected component is not supported on these operating system versions.

Windows NT Server 4.0, Windows 2000 Server, and Windows Server 2003 are at a reduced risk from this vulnerability because the affected component is not installed by default. Even if Internet Information Services (IIS) is installed, the affected component is not installed by default.

Exchange 2000 servers and systems that have manually enabled NNTP are primarily at risk from this vulnerability. Exchange 2000 Server and Exchange Server 2003 require the installation of the affected operating system component. However upon installation, Exchange Server 2003 disables the affected operating system component. Exchange Server 2003 requires an administrator to manually re-enable this component to become vulnerable to this issue. Exchange 2000 Server does not disable this component by default when it is installed. However, if an administrator manually disables this component after installing Exchange Server 2000, the system is not vulnerable to this issue. Best practice recommendations for helping to secure Exchange 2000 Server include disabling the affected operating system component. For more information about how to help secure Exchange 2000 Server, visit the following

<<http://www.microsoft.com/technet/security/guidance/secmod43.mspx>> Web site.

I use Windows NT Server 4.0 Terminal Server Edition Service Pack 6. Could I be affected by this vulnerability ?

No. The NNTP component ships as part of the Windows NT 4.0 Option Pack. The Windows NT 4.0 Option Pack is not supported on this operating system version. For more information, see Microsoft Knowledge Base Article <<http://support.microsoft.com/?kbid=190157>> 190157.

If NNTP is installed and running, is it vulnerable ?

Yes, except for the Exchange 5.5 Server version of the NNTP Component.

Is Exchange 5.5 Server affected by this vulnerability ?

Exchange 5.5 Server and Exchange 5.0 Server are not affected by this vulnerability. Their implementation of NNTP is independent of the implementation in other affected software versions.

Securiteam: [NT] Vulnerability in NNTP Allows Remote Code Execution (MS04-036)

Could the vulnerability be exploited over the Internet ?

Yes. An attacker may be able to exploit this vulnerability over the Internet.

I visit news servers frequently from my home computer. Does this vulnerability affect me ?

No. It only affects servers that offer NNTP services; it does not affect the client systems that visit them.

What does the update do ?

The update removes the vulnerability by modifying the way that the NNTP component validates the length of a message before it passes the message to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed ?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information indicating that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited ?

No. Microsoft had not received any information indicating that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS04-036.msp>>

<http://www.microsoft.com/technet/security/bulletin/MS04-036.msp>

The original article can be found at:

<<http://www.securiteam.com/windowsntfocus/6T00C0UBGU.html>>

<http://www.securiteam.com/windowsntfocus/6T00C0UBGU.html>

=====

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,

Securiteam: [NT] Vulnerability in NNTP Allows Remote Code Execution (MS04-036)

loss of business profits or special damages.