

[NT] NNTP Service in Windows Contains Memory Leak

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0067.html>

From: support@securiteam.com

Date: 08/15/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] NNTP Service in Windows Contains Memory Leak

Message-Id: <20010815195557.A4D10138BF@mail.der-keiler.de>

Date: Wed, 15 Aug 2001 21:55:57 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

NNTP Service in Windows Contains Memory Leak

SUMMARY

The NNTP (Network News Transport Protocol) service in Windows NT 4.0 and Windows 2000 contains a memory leak in a routine that processes news postings. Each time such a posting is processed that contains a particular construction, the memory leak causes a small amount of memory to no longer be available for use. If an attacker sent a large number of posts, the server memory could be depleted to the point at which normal service would be disrupted. An affected server could be restored to normal service by rebooting.

DETAILS

Affected Software:

- * Microsoft Windows NT 4.0
- * Microsoft Windows 2000

Mitigating factors:

- * Windows NT 4.0 does not contain a native NNTP service. NNTP is only available on the system if the Windows NT 4.0 Option Pack has been

Securiteam: [NT] NNTP Service in Windows Contains Memory Leak

installed.

* The default configuration of NNTP is not affected by the vulnerability, as no newsgroups are configured by default.

* The vulnerability would not enable an attacker to usurp any administrative control or compromise data on the machine.

Patch availability:

Download locations for this patch

* Windows NT 4.0 Server and Server, Enterprise Edition:

<<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31955>>
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31955>

* Windows 2000 Server and Advanced Server:

<<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31925>>
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31925>

* Microsoft Windows 2000 Datacenter Server:

Patches for Windows 2000 Datacenter Server are hardware-specific and available from the original equipment manufacturer.

What's the scope of this vulnerability?

This is a denial of service vulnerability. By repeatedly sending a news posting to an affected server, an attacker could degrade its performance, potentially to the point where the server would be unable to provide useful service.

The vulnerability would not enable an attacker to compromise any data on the server, or to usurp any privileges on the machine. The administrator of an affected Windows NT 4.0 machine could restore normal service by rebooting the machine; a Windows 2000 machine would automatically restore service.

What causes the vulnerability?

The vulnerability results because the NNTP service in Windows NT 4.0 and Windows 2000 contains a memory leak. If a sufficient quantity of posting containing a particular malformation were received, it could deplete the available memory to the point where the server would be incapable of performing useful work.

What's NNTP?

NNTP (Network News Transfer Protocol) is an industry-standard protocol that specifies a method for posting, distributing, searching, and archiving news articles via Internet-based servers. The vulnerability results because the NNTP implementation in Windows NT 4.0 and Windows 2000 contains a memory leak that could be used to disrupt the NNTP service.

What's a memory leak?

A memory leak is an implementation error that depletes the available memory on a system. As a process on a computer runs, it may need more or less memory, depending on exactly what it is doing from one minute to the next. When the process needs more memory, it requests it from the operating system; when it no longer needs the additional memory, it should return it to the operating system so it can be allocated to other

Securiteam: [NT] NNTP Service in Windows Contains Memory Leak

processes.

A memory leak occurs when a process does not correctly return memory to the operating system. Instead of becoming available for allocation to another process, the memory remains assigned to the process even though the process is no longer using it. This effectively makes the block of memory unavailable.

How does the memory leak happen in this case?

In the case of this vulnerability, the NNTP service has a memory leak that results when it processes a particular type of malformed news posting. Each time the service accepts such a posting, it requests memory from the operating system; however, it does not return the memory when it finishes handling the request.

What could an attacker do via this vulnerability?

An attacker could repeatedly send malformed news postings to an affected server in order to deplete its pool of available memory. As the server's memory pool was depleted, its performance would gradually slow. If the attack were sustained for a long enough period, the server could potentially be brought to a standstill and be unable to perform useful work.

Does the NNTP service run by default?

The answer varies by operating system.

* Default installations of Windows NT 4.0 do not contain an NNTP service. NNTP support is included as part the Windows NT 4.0 Option Pack. If the Option Pack has been installed, NNTP runs by default.

* In Windows 2000 server products, NNTP is a native service, and it does run by default. In Windows 2000 Professional, NNTP is neither installed nor running by default.

However, this is not the complete answer. It is not enough for the NNTP service to be installed and running – it also has to be configured to accept postings. By default, the NNTP service does not have any newsgroups configured, so it does not accept any postings and hence is not affected by the vulnerability. It is only if the service is running and configured to accept postings that it is vulnerable.

Would a successful attack via this vulnerability only disrupt NNTP services, or would other services on the system be affected as well?

Because the vulnerability depletes the memory pool that all services on the machine use, a successful attack via the vulnerability would affect the operation of all services on the machine, not just the terminal services. Therefore, for instance, if the machine also hosted shared files, users might be unable to access them after the machine had been attacked.

Would this vulnerability enable the attacker to gain any privileges on the machine?

No. The sole effect of a successful attack via this vulnerability would be

Securiteam: [NT] NNTP Service in Windows Contains Memory Leak

to prevent the server from operating normally. It would not grant any privileges to the attacker, nor would it allow any data to be compromised.

How could an affected server be put back into service?

The server could be returned to normal service by rebooting it.

Could this vulnerability be exploited from the Internet?

The vulnerability could be exploited by any user who could send postings to it. If the server accepts postings from the Internet, an Internet user could exploit the vulnerability.

I run an NNTP server, but it is a "push" server that does not allow users to post to it. Is my server at risk?

No. If your server does not accept postings, an attacker could not cause the memory leak to happen.

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

No. The vehicle, by which the NNTP service ships, the Windows NT 4.0 Option Pack, cannot be installed on terminal servers.

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 machines that visit them.

What does the patch do?

The patch eliminates the vulnerability by causing the NNTP service in Windows NT 4.0 and Windows 2000 to properly deallocate memory after processing a news posting.

ADDITIONAL INFORMATION

The information has been provided by <mailto:secnotif@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.

Securiteam: [NT] NNTP Service in Windows Contains Memory Leak

- *Previous message:* support@securiteam.com: "[\[UNIX\] SIX-Web board "Show Files" Vulnerability](#)"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)