

# [NT] Microsoft Telnet Client Allows Information Disclosure (MS05-033)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0065.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 06/15/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 15 Jun 2005 16:13:03 +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>

-----

Microsoft Telnet Client Allows Information Disclosure (MS05-033)

---

## SUMMARY

<<http://www.ietf.org/rfc/rfc0854.txt>> Telnet is an industry standard protocol that allows a user to establish a remote terminal session on a telnet server. Because this is a terminal session, there is only a command-line interface. Telnet is mainly used for simple remote administration at a command prompt. This is a separate application than Microsoft HyperTerminal. Microsoft HyperTerminal is not affected by this issue.

An attacker who successfully exploited Microsoft's Telnet client information disclosure vulnerability could remotely read the session variables for users who have open connections to a malicious telnet server.

## DETAILS

Vulnerable Systems:

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B8BA775E-E9A7-47E9-81A9-A68A71B9FAAC>>

Securiteam: [NT] Microsoft Telnet Client Allows Information Disclosure (MS05-033)

Download the update

\* Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C6161D9E-1672-479E-8BAF-754A64DFAB47>>

Download the update

\* Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium) <>

Download the update

\* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B281550B-8FAE-4FF3-9BB7-E4BA325779B9>>

Download the update

\* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=22095E78-A559-40EA-8B65-9C727F4E752F>>

Download the update

\* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C23A4E16-E228-4A80-A4CB-9DCEF462B97A>>

Download the update

\* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=DCC6840F-E626-4266-A63A-CDDEC0EC44D6>>

Download the update

\* Microsoft Windows Services for UNIX 3.5 when running on Windows 2000

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7c3dd615-b82d-4520-9c3a-376283b01d5b>>

Download the update

\* Microsoft Windows Services for UNIX 3.0 when running on Windows 2000

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8eaad650-54db-44bc-ac9b-fc8a50f5a3b5>>

Download the update

\* Microsoft Windows Services for UNIX 2.2 when running on Windows 2000

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=32c4e286-2c4d-491a-9e05-4ca0b055d5dc>>

Download the update

Immune Systems:

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

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

An attacker who successfully exploited this vulnerability could remotely read the session variables of users who have open connections to a malicious telnet server. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly. It could be used to produce useful information to try to further compromise the affected system.

What is Microsoft Windows Services for UNIX?

<<http://www.microsoft.com/windows/sfu/productinfo/overview/default.asp>>

Microsoft Windows Services for UNIX is a product that allows customers to run UNIX application on a Windows system. Providing this capability expands support for UNIX applications, daemons, and scripts by providing an enhanced UNIX environmental subsystem beyond the standard POSIX subsystem. Windows Service for UNIX allows customers to run UNIX applications, daemons, and scripts.

How could an attacker exploit the vulnerability?

There are several different ways that an attacker could attempt to exploit this vulnerability. However, user interaction is required to exploit this vulnerability in every case. Here are some examples:

- \* An attacker could host a malicious Web site that is designed to exploit this vulnerability through Internet Explorer and then persuade a user to view the Web site.

- \* An attacker could also create an e-mail message that has a specially crafted Telnet URL. An attacker could attempt to exploit this vulnerability by persuading the user to view or to preview an e-mail message than contains a Telnet URL and then persuade the user to then click the Telnet URL.

What systems are primarily at risk from the vulnerability?

All affected operating systems are at risk from this vulnerability.

However, an attacker would have to combine this issue with another vulnerability for a system to be at risk.

Mitigating Factors for Telnet Vulnerability – CAN-2005-1205:

- \* In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's Web site.

- \* An attacker who successfully exploited this vulnerability could only read the session variables for the affected user. This does not include critical data such as password hashes.

- \* All versions of Windows Services for UNIX are vulnerable to this issue only when they are running on Windows 2000. When Windows Services for UNIX is running on other operating systems, it is not vulnerable to this issue.

Workarounds for Telnet Vulnerability – CAN-2005-1205:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

- \* Un-register the default Telnet client:

To help prevent attacks that use Telnet URLs, you can remove the Telnet,

Securiteam: [NT] Microsoft Telnet Client Allows Information Disclosure (MS05-033)

Tn3270, and Rlogin handlers. This will prevent Internet Explorer and other applications from automatically launching Telnet sessions.

Note Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend that you back up the registry before you edit it.

1. Click Start, click Run, type "regedt32" (without the quotation marks), and then click OK.
2. In Registry Editor, delete the following registry keys:

HKEY\_CLASSES\_ROOT\telnet\shell\open\command  
HKEY\_CLASSES\_ROOT\tn3270\shell\open\command  
HKEY\_CLASSES\_ROOT\rlogin\shell\open\command

Impact of Workaround: These changes will help prevent attacks by blocking Telnet from being used to process Telnet, Tn3270, or Rlogin URLs.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1205>>  
CAN-2005-1205

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-033.msp>>  
<http://www.microsoft.com/technet/security/Bulletin/MS05-033.msp>

=====

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.