

# [NT] Vulnerability in Telephony Service Allows Remote Code Execution (MS05-040)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0040.html>

---

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

*Date:* 08/10/05

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

Date: 10 Aug 2005 14:55:28 +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 Telephony Service Allows Remote Code Execution (MS05-040)

---

## SUMMARY

A vulnerability exists in the Telephony Application Programming Interface (TAPI) service that could allow remote code execution.

## DETAILS

Vulnerable Systems:

\* Microsoft Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C7417EA1-7AFC-4A55-95DC-E814975B8AE6>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B049004B-AF28-41D7-8AE6-7A3DB15211F1>>

Download the update

\* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=705545D0-B53B-4E17-8B62-A4C652697C61>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0097FE14-1D6B-4423-A437-DEA1ED665A07>>

## Securiteam: [NT] Vulnerability in Telephony Service Allows Remote Code Execution (MS05-040)

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=BC16BEAE-0BAD-490C-A80F-4BF81C360CA0>>

Download the update

\* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0CEF9CC2-A7BD-42E0-81B1-EDC303DA8A40>>

Download the update

\* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME) Review the FAQ section of this bulletin for details about these operating systems.

### Telephony Service Vulnerability – CAN-2005-0058

A remote code execution vulnerability exists in Telephony Application Programming Interface (TAPI) that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

### Mitigating Factors for Telephony Service Vulnerability – CAN-2005-0058:

Remote code execution is possible if you have manually enabled the telephony server feature. The telephony server feature is only available on Windows 2000 Server and Windows Server 2003. For information about this feature, visit the following

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/a3574189-fd2f-4e12-90d9-Web site>>

On Windows Server 2003 the Telephony service is restricted to authenticated user accounts, even when enabled as a telephony server. Anonymous attacks are not possible on Windows Server 2003.

On Windows 2000 Server and Windows Server 2003 based systems that have not manually configured the telephony server feature, this is a local elevation of privilege vulnerability. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.

On Windows 2000 Professional and on Windows XP, this is a local elevation of privilege vulnerability. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.

By default, the Telephony service is not running on Windows XP and Windows Server 2003. However, the TAPI client will start the Telephony service without user interaction when required. Unless the Telephony service has been set to Disabled by an administrator, a non-privileged user account can start this service. Systems that have disabled the Telephony service would not be vulnerable to this issue.

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

## Securiteam: [NT] Vulnerability in Telephony Service Allows Remote Code Execution (MS05-040)

Internet have a minimal number of ports exposed.

Workarounds for Telephony Service Vulnerability – CAN-2005-0058: 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.

Disable the Telephony service.

Disabling the Telephony service will help protect the affected system from attempts to exploit this vulnerability. To disable the Telephony service, follow these steps:

1. Click Start, and then click Control Panel. Alternatively, Click Start, point to Settings, and then click Control Panel.
2. Double-click Administrative Tools.
3. Double-click Services.
4. Double-click Telephony.
5. In the Startup type list, click Disabled.
6. Click Stop, and then click OK.

You can also stop and disable the Telephony service by using the following command at the command prompt:

```
sc stop tapisrv & sc config tapisrv start= disabled
```

Impact of Workaround: If the Telephony service is disabled, any dependant services or operating system features would fail. Examples of these features include the new connection wizard, RAS, modem based dial-up networking, and the fax service, would fail. Therefore, we recommend this workaround only on systems that cannot apply the security update.

Block the following at the firewall:

- \* UDP ports 135, 137, 138, and 445, and TCP ports 135, 139, 445, and 593
- \* All unsolicited inbound traffic on ports greater than 1024
- \* Any other specifically configured RPC port

These ports are used to initiate a connection with RPC. RPC can be used to remotely communicate with the Telephony service on Windows 2000 Server and Windows Server 2003. Blocking them at the firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. Also, make sure that you block any other specifically configured RPC port on the remote 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 ports that RPC uses, visit the following <http://go.microsoft.com/fwlink/?LinkId=21312> Web site.

To help protect from network-based attempts to exploit this vulnerability, use a personal firewall, such as the <http://go.microsoft.com/fwlink/?LinkId=33335> Internet Connection

## Securiteam: [NT] Vulnerability in Telephony Service Allows Remote Code Execution (MS05-040)

Firewall, which is included with Windows Server 2003.

By default, the Internet Connection Firewall feature in Windows Server 2003 helps protect your Internet connection by blocking unsolicited incoming traffic. We recommend that you block all unsolicited incoming communication from the Internet.

To enable the Internet Connection Firewall feature by using the Network Setup Wizard, follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Network and Internet Connections, and then click Setup or change your home or small office network. The Internet Connection Firewall feature is enabled when you select a configuration in the Network Setup Wizard that indicates that your system is connected directly to the Internet.

To configure Internet Connection Firewall manually for a connection, follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Networking and Internet Connections, and then click Network Connections.
3. Right-click the connection on which you want to enable Internet Connection Firewall, and then click Properties.
4. Click the Advanced tab.
5. Click to select the Protect my computer or network by limiting or preventing access to this computer from the Internet check box, and then click OK.

Note If you want to enable certain programs and services to communicate through the firewall, click Settings on the Advanced tab, and then select the programs, the protocols, and the services that are required.

To help protect from network-based attempts to exploit this vulnerability, enable advanced TCP/IP filtering on systems that support this feature.

You can enable advanced TCP/IP filtering to block all unsolicited inbound traffic. For more information about how to configure TCP/IP filtering, see <<http://support.microsoft.com/kb/309798>> Microsoft Knowledge Base Article 309798.

To help protect from network-based attempts to exploit this vulnerability, 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 about how to apply filters is available in <<http://support.microsoft.com/kb/313190>> Microsoft Knowledge Base Article 313190 and <<http://support.microsoft.com/kb/813878>> Microsoft Knowledge Base Article 813878.

## Securiteam: [NT] Vulnerability in Telephony Service Allows Remote Code Execution (MS05-040)

<FAQ for Telephony Service Vulnerability – CAN-2005-0058:> FAQ for Telephony Service Vulnerability – CAN-2005-0058:

What is the scope of the vulnerability?

This can be a remote code execution vulnerability or a <<http://go.microsoft.com/fwlink/?LinkId=21142>> local privilege elevation vulnerability, depending on the operating system version and configuration. See the What systems are primarily at risk from the vulnerability? questions in the FAQ section for more information. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

What causes the vulnerability?

The process that the Telephony service uses to validate data and permissions.

What is the Telephony service?

The Telephony service provides support for Telephony Application Programming Interface (TAPI). TAPI integrates telecommunications with the operating system. TAPI supports both traditional and IP telephony to provide voice, data, and video communication. Supported hardware includes sound and video cards, modems, ISDN lines, ATM networks, and cameras. By using this hardware, you can communicate over direct connections to local computers, telephone lines, LANs, WANs, and the Internet.

In addition to making and receiving calls, programs can use TAPI to provide enhanced telephony features such as caller ID, call routing, voice mail, and video conferencing. Communication programs may identify the caller, recall and display caller information, and even prioritize or route a call, based on customer information. For more information about TAPI, visit the following

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/7d644322-d216-484c-ab74>> Web site.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

Who could exploit the vulnerability?

On Windows 2000 Server, any anonymous user who could deliver a specially crafted message to the affected system could try to exploit this vulnerability.

On Windows Server 2003, the Telephony service is restricted to authenticated user accounts.

On Windows 2000 Professional and on Windows XP, this is a local elevation of privilege vulnerability. To try to exploit the vulnerability, an attacker must be able to log on locally to a system and run a program on Windows 2000 Professional and Windows XP.

## Securiteam: [NT] Vulnerability in Telephony Service Allows Remote Code Execution (MS05-040)

What systems are primarily at risk from the vulnerability?

Windows 2000 Servers that are configured as telephony servers are primarily at risk from anonymous attackers. However, an administrator must take steps to configure a Windows 2000 Server computer as a telephony server. To see these steps, visit the following

<[http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/TAPI\\_s](http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/TAPI_s)> Web site.

Windows Server 2003 systems that configured as telephony servers are at risk from authenticated attackers. However, an administrator must take steps to configure a Windows Server 2003 computer as a telephony server.

To see these steps, visit the following

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/a3574189-fd2f-4e12-90d9->> Web site.

On systems that have not been configured as a telephony server, on Windows 2000 Professional, and on Windows XP, this is a local elevation of privilege vulnerability.

Systems that have disabled the Telephony service are not vulnerable to this issue.

Are Windows 98, Windows 98 Second Edition or Windows Millennium Edition critically affected by this vulnerability?

No. Although Windows 98, Windows 98 Second Edition, and Windows Millennium Edition do contain the affected component, the vulnerability is not critical. For more information about severity ratings, visit the following

<<http://go.microsoft.com/fwlink/?LinkId=21140>> Web site.

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your PC. End users can visit the

<<http://go.microsoft.com/fwlink/?LinkId=21169>> Protect Your PC Web site.

IT professionals can visit the

<<http://go.microsoft.com/fwlink/?LinkId=21171>> Security Guidance Center Web site.

What does the update do?

The update removes the vulnerability by modifying the way that Telephony service 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 to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

Securiteam: [NT] Vulnerability in Telephony Service Allows Remote Code Execution (MS05-040)

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

No. Microsoft had not received any information to indicate 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.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0058>>  
CAN-2005-0058

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/MS05-040.msp>>  
<http://www.microsoft.com/technet/security/Bulletin/MS05-040.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.