

# [NT] NULL Sessions Vulnerabilities Using Alternate Named Pipes

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0033.html>

---

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

*Date:* 07/11/05

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

Date: 11 Jul 2005 19:33:14 +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>

-----

NULL Sessions Vulnerabilities Using Alternate Named Pipes

---

## SUMMARY

By taking advantage of hardcoded named pipes allowed for NULL sessions and using the property of MSRPC that, by default, all available RPC interfaces in a process can be reached using any opened endpoint, it is possible to anonymously enumerate Windows services and read the Application and System eventlogs.

## DETAILS

Vulnerable Systems:

\* Windows NT 4.0, Windows 2000 prior to URP1 for Windows 2000 SP4

Windows XP and Windows Server 2003 are not directly affected by the vulnerabilities described in this document.

Still, the alternate named pipes technique also applies to Windows XP and Windows Server 2003, including Windows XP SP2 and Windows Server 2003 SP1.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2150>>  
CAN-2005-2150

## Securiteam: [NT] NULL Sessions Vulnerabilities Using Alternate Named Pipes

Anonymous Windows service enumeration:

The svcctl MSRPC interface is used to communicate with the  
<[http://www.hsc.fr/ressources/articles/win\\_net\\_srv/ch04s07s09.html](http://www.hsc.fr/ressources/articles/win_net_srv/ch04s07s09.html)>  
Windows SCM (Service Control Manager).

The svcctl vulnerability allows an anonymous user to connect to the SCM (Service Control Manager). It is then possible to enumerate installed or running services. See image at:

<[http://www.hsc.fr/ressources/presentations/null\\_sessions/img16.html](http://www.hsc.fr/ressources/presentations/null_sessions/img16.html)>  
[http://www.hsc.fr/ressources/presentations/null\\_sessions/img16.html](http://www.hsc.fr/ressources/presentations/null_sessions/img16.html)

Depending on the security descriptor protecting each service (stored in binary under the Security registry subkey of each service's subkey), it might be possible to anonymously start or even stop a Windows service. Because in Windows NT 4.0 and Windows 2000, the EVERYONE group contains the ANONYMOUS LOGON SID, a service with a weak DACL allowing members of the EVERYONE group to start (or stop) the service can be remotely started or stopped anonymously.

For more information about services permissions, see  
<<http://cert.uni-stuttgart.de/archive/bugtraq/2004/10/msg00159.html>>  
<http://cert.uni-stuttgart.de/archive/bugtraq/2004/10/msg00159.html>

Anonymous Application and System eventlogs read:

The <[http://www.hsc.fr/ressources/articles/win\\_net\\_srv/ch04s07s06.html](http://www.hsc.fr/ressources/articles/win_net_srv/ch04s07s06.html)>  
eventlog MSRPC interface is used to communicate with the Windows eventlog service. The eventlog vulnerability can be used to anonymously read either the Application or System eventlog of a remote Windows NT 4.0 or Windows 2000 system.

It is not possible to read the Security eventlog because a specific Windows privilege must be held by the caller process (SeSecurityPrivilege).

Vendor Status:

Both vulnerabilities are fixed in the URPI for Windows 2000 SP4 recently released by the vendor: <<http://support.microsoft.com/kb/900345/>>  
<http://support.microsoft.com/kb/900345/>

The svcctl vulnerability was fixed by modifying the SCM DACL (enforced when the OpenSCManager{A,W} operation is used), denying access for the ANONYMOUS LOGON SID.

The eventlog vulnerability was fixed by using a RPC callback function for the eventlog interface, to reject unauthenticated binds.

Workarounds:

It is possible to protect against the eventlog vulnerability by adding and setting to 1 the RestrictGuestAccess registry value, under the following two registry keys:

HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\  
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\System\

In Windows 2000, the RestrictGuestAccess value can be set using the following security options:

## Securiteam: [NT] NULL Sessions Vulnerabilities Using Alternate Named Pipes

- \* Restrict guest access to application log
- \* Restrict guest access to system log

These settings are mentioned in the following article:

<<http://support.microsoft.com/kb/842209>>  
<http://support.microsoft.com/kb/842209>

It is recommended to set these registry values on Windows NT 4.0 systems, where no other workaround is available.

Vulnerability Assessment:

svcctl vulnerability:

<<http://www.nessus.org/plugins/index.php?view=single&id=18585>>  
<http://www.nessus.org/plugins/index.php?view=single&id=18585>

eventlog vulnerability:

<<http://www.nessus.org/plugins/index.php?view=single&id=18602>>  
<http://www.nessus.org/plugins/index.php?view=single&id=18602>

For more information, see the following documents:

- \* <[http://www.hsc.fr/ressources/presentations/null\\_sessions/](http://www.hsc.fr/ressources/presentations/null_sessions/)> MSRPC null sessions: exploitation and protection
- \* <[http://www.hsc.fr/ressources/articles/win\\_net\\_srv/](http://www.hsc.fr/ressources/articles/win_net_srv/)> Windows network services internals

Disclosure Timeline:

2004/01/23: Vulnerability reported to vendor

2004/02/12: Vendor announces its intention to release fixes as part of the next Windows 2000 Service Pack

2004/09/09: A related vulnerability affecting Windows XP SP2 is published

2005/02/08: Release of MS05-007, fixing a specific instance of a similar vulnerability in Windows XP and Windows XP SP2

2005/02/28: Private versions of Windows 2000 fixes available for test

2005/03/30: Confirmation that tested fixes correct the vulnerability

2005/06/28: Release of URP1 for Windows 2000 SP4, which includes fixes for Windows 2000

### ADDITIONAL INFORMATION

The information has been provided by

<<mailto:Jean-Baptiste.Marchand@hsc.fr>> Jean-Baptiste Marchand.

The original article can be found at:

<[http://www.hsc.fr/ressources/presentations/null\\_sessions/](http://www.hsc.fr/ressources/presentations/null_sessions/)>  
[http://www.hsc.fr/ressources/presentations/null\\_sessions/](http://www.hsc.fr/ressources/presentations/null_sessions/)

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

## Securiteam: [NT] NULL Sessions Vulnerabilities Using Alternate Named Pipes

### 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.