

Re: [Full-Disclosure] DCOM RPC exploit (dcom.c)

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-07/1048.html>

From: Jason (security_at_brvenik.com)

Date: 07/27/03

To: Paul Schmehl <pauls@utdallas.edu>

Date: Sun, 27 Jul 2003 17:23:45 -0400

Paul Schmehl wrote:

> *On Sun, 2003-07-27 at 14:24, Jason wrote:*

>

>> *Ok:*

>> *In short it goes like this.*

>>

>> *Click Start->Run*

>> *Type "dcomcnfg.exe"*

>> *Turn it off*

>

>

> *Great! Now go click all 5000 computers we have to take care of. This is exactly what I'm talking about. You smugly criticize networks for not fixing problems, yet you completely ignore the fact that the tools to do this on an enterprise scale either don't exist, are far too expensive for the average network or require scripting expertise that most don't have. Not to mention the fact that for this to even work, the security context must be administrator and the concept of sudo hasn't entered the Windows world in a secure implementation (that I'm aware of).*

>

Pg 189 of the document located at the link previously provided. The link is included here again for convenience.

<http://downloads.securityfocus.com/library/S24NTSec.doc>

Interestingly it makes use of a free program for windows available at

<http://www.kixtart.org/>

---- snip ----

:SECREG29

; If you are absolutely certain that you have clients that are NOT using DCOM,

; use this edit. Read the COM Security whitepaper or MSKB Article Q158508 for

Full-Disclosure: Re: [Full-Disclosure] DCOM RPC exploit (dcom.c)

; further details.

\$DSCRIPTN = "Disable DCOM"

\$LEVEL = "3"

\$REGKEY = "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole"

\$REGVALUE = "EnableDCOM"

\$REGTYPE = "REG_SZ"

\$GOOD = "N"

\$BAD = "Y"

\$SPECIAL = "0"

\$NEXT = SECREG30

GOTO CHECKSEC

--- snip ---

>>Please see references above for the counter to this statement.

Here are the references again in case someone missed them.

<http://www.uksecurityonline.com/husdg/wxpp2.php>

<http://downloads.securityfocus.com/library/S24NTSec.doc>

<http://www.microsoft.com/technet/treeview/?url=/technet/security/topics/hardsys/>

<http://www.darknet.org.uk/content/files/securewin2k.txt>

http://www.giac.org/practical/GSEC/Trevor_Cuthbert_GSEC.pdf

>>

>>As to charging for the knowledge. Yeah, it is my time and my mind that
>>does the work, of course I am going to charge for it. Does UT provide an
>>education for free to everyone?

>>

>

> No, but we don't charge them an arm and leg either. Like most
> universities, the product we provide is bargain priced and available to
> almost anyone that's alive and breathing.

>

>>Hardly hypocritical, the information is free for the taking and the
>>tools are readily available. Most of them already exist in the OS that
>>was paid for. It simply requires that the time be put in to do it.

>>

>>To the open source easy to use statement, since windows is pay to use
>>why would anyone expect to be able to manage it for free?

>

>

> I don't think it's unreasonable to expect an operating system to come
> with the tools to manage it on an enterprise level rather than having to
> spend extra dollars for that functionality. Do you?

There is a difference between the tools to manage it easily and the
tools to manage it. The tools are there to automate this and many other
changes.

basic instructions.

Full-Disclosure: Re: [Full-Disclosure] DCOM RPC exploit (dcom.c)

```
Start->Run [cmd|command]
cd \my\netlogon\share
edit netlogon.bat
@import_sec_reg_keys.bat
Alt->F->X->Yes
```

```
>
>
>> I vote to
>>spend my time making the free things easier to use so I do not have to
>>buy windows.
>>
>
> Then don't criticize the Windows "community" for not having the tools to
> do the job. Criticize Microsoft.
```

I criticized no one. I stated that I will spend my time elsewhere.

```
>
>>I live in the real world, it is harsh and brutal, it is in fact the same
>>world we all live in. Unfortunately the universities are half the
>>problem here. A fantasy world exists on every campus where the belief is
>>that everything should be free and you should be able to do what ever
>>you want.
>
>
> You're sadly mistaken. Unis don't expect to get everything for free.
> But they don't get enough funding to purchase a full set of commercial
> tools either. And where do you think a large chunk of the open source
> stuff comes from anyway? Who writes much of the code? Who provides the
> mirrors to the world, free of charge? Who does most of the research?
>
```

If the "Unis" do all this work for free (hardly, my taxes pay for it) and play such a huge role then maybe they could do a little research as a team and make it "Easy" to run windows.

```
>
>> Only one catch, we charge to be here at university to have
>>access to our fantasy world where you get this information and do what
>>you want but we want you to give your information to us for free even if
>>you are not in our fantasy world. That is hypocritical.
>>
>
> It would be, if that were reality. The reality is that most people's
> education is highly subsidized by governments and private contributors.
> If students actually had to *pay* for their education (what it actually
> costs to provide it to them) there would be far fewer students, far
> fewer universities and a lot less open source programs.
>
```

Full-Disclosure: Re: [Full-Disclosure] DCOM RPC exploit (dcom.c)

Yuppers, my tax dollars combined with many others tax dollars enable this subsidy that in turn enables this "free" stuff. Now I wonder, did I contribute to your education or just your continued employment?

>>>Here we go again with this fantasy stuff, the information is free, the
>>>work to implement it is yours to do.
>
>
> Funny how you think **your* labor has value, but the IT admins' does not.*
>

Hardly my position. I never stated my labor has value and the IT admins labor does not. I did state "I will charge a fair price for a fair days work" If that implies that my time has value and admin time does not then I suggest it is time to evaluate either the fair price being charged or the fair days work being delivered.

Attempting to put words into my mails and twist my statements to support your position will not work.

I have only provided my research services for free to this list so that all may read the excellent works produced by others and published for free in the hopes that the next time this type of pending event arrives it may become a non event. Sounds to me like my time has less value because I gave it away for free.

>
>>>IDSes don't protect anything. They merely tell you where the shit just
>>>hit the fan. IPSes are still in their infancy, and very few admins are
>>>going to trust them to stop bad stuff without also stopping important
>>>traffic.
>>
>>Some select quotes from any dictionary. They seem to apply to IDS in
>>this case.
>>
>>protect: To keep from being damaged, attacked, stolen, or injured; guard.
>>
>>guard: To protect from harm by or as if by watching over.
>> To supervise entry or exit through; keep watch at.
>>
>>
>
> Oh, I get it. You've never actually used an IDS. You just understand
> the dictionary definition of one. Try sitting in front of the console
> staring at a half a million alerts and see if the IDS **does** anything
> besides spewing information that **you** have to research, that **you**
> have to interpret and that **you** have to take action on.
>

All this reminds me of a quote. I cannot recall the orgin unfortunately.

Full-Disclosure: Re: [Full-Disclosure] DCOM RPC exploit (dcom.c)

"never argue with idiots, they will drag you down and beat you with experience"

Sounds like a case of the pending Mondays to me. Do this, turn off the IDS and try not having it to catch you when the fan starts spreading dung. Then try to fix the situation at hand and become proof positive of Darwin's Theory.

Houston, we have reached the experience part of this discussion.

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>