

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

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-07/1041.html>

From: Jason (security_at_brvenik.com)

Date: 07/27/03

To: Paul Schmehl <pauls@utdallas.edu>

Date: Sun, 27 Jul 2003 15:24:56 -0400

Paul Schmehl wrote:

> *On Sat, 2003-07-26 at 23:22, Jason wrote:*

>

>> *The war begins...*

>>

>> *I'm not going to debate the release of code with anyone. Simply put,*

>> *best practices should have mitigated this in a huge way from the*

>> *beginning. All of the remaining threat should have been tested and*

>> *patched by now.*

>>

>

> *What a polyanna world you live in.*

>

>

>> *RPC services have been a risk forever. Knowing that the majority of*

>> *clients do not use DCOM, an RPC service, is all that the administrators*

>> *needed to know. Do you build a *nix system and leave all(any) RPC*

>> *services enabled?*

>>

>> *** DCOM should have been disabled for 99% of the systems they have. ***

>>

>

> *So, since you're so smart, publish a document that explains, in language*

> *Windows users can understand, how to disable DCOM. Oh, and make sure*

> *you include the code so the fix can be deployed to thousands of machines*

> *easily, just like the worms are.*

Ok:

In short it goes like this.

Click Start->Run

Type "dcomcnfg.exe"

Turn it off

Why would I write any more? It is nothing new and free to have already.

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

<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

>
> *ISTM the "security community" is a lot more eager to publish exploits*
> *than they are to publish fixes – unless you want to pay them obscene*
> *consultant fees. It's interesting that many seek fame by releasing and*
> *publishing exploits, but then they want to charge for the knowledge to*
> *fix the problem. (And no, I don't need your help.)*

Please see references above for the counter to this statement.

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?

>
> *If I had millions of dollars, I could put all sorts of "security*
> *solutions" in place. I have yet to find one that is reasonably priced*
> *(for Windows.) I have vendors calling me every week offering the next*
> *great security solution for "only" \$100,000 or more.*
>
> *Have you noticed how the open source community doesn't do much*
> *development for Windows? (I'm talking about security products here.)*
> *It's getting better, with snort, nessus and nmap leading the way, but*
> *where are the open source tools for patch deployment for Windows? Where*
> *are the open source tools for checking patch levels and verifying*
> *compliance? (And please don't tell me hfnetchk.) Far too many open*
> *source developers sneer at Windows and refuse to even develop for it,*
> *then turn around and criticize the Windows admins for not maintaining*
> *their boxes properly and having a lax attitude about security. Seems*
> *grossly hypocritical to me.*

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 vote to spend my time making the free things easier to use so I do not have to buy windows.

>
>
>> *Ohhh, now we are going to complain about having to put in all those*
>> *extra hours and spend all that overtime money. Umm, be happy you still*
>> *have a job.*
>>

>
> *Overtime money? You must be kidding. Our IT people work an average of*
> *60 hours a week and get no overtime money. They're all on salary and*
> *"exempt" from overtime pay. The reason I have this Gentoo box at home*
> *is so I can monitor the network when I'm "not working". (I'm not*
> *complaining, mind you, I happen to love what I do.)*
>
> *While the rest of the university community is enjoying their two week*
> *Christmas holiday, the IT staff is busily patching and doing maintenance*
> *on boxes that are too critical to take down during the academic year.*
>
> *Please visit the real world some day. It might actually change your*
> *viewpoint. (Then again, maybe not, since you are so far into the*
> *fantasy world.)*
>

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. 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.

>
>> *Sorry, no sympathy here.*
>>
>> *** If you have assets worth protecting you hire people who are capable*
>> *of protecting them. ***
>>
>
> *Assuming, of course, that you have the money to do so. Wouldn't be nice*
> *if your imaginary scenarios could actually play out in real life. In*
> *real life IT is almost always understaffed and overworked – and then we*
> *have to suffer the "experts" telling us what a lousy job we're doing and*
> *how much better off we'd be if we'd simply hire them – at outrageously*
> *inflated consulting fees – to fix our problems.*

Here we go again with this fantasy stuff, the information is free, the work to implement it is yours to do. I accuse nobody of doing a horrible job nor do I try to charge outrageous fees to make the accusation. I will charge a fair price for a fair days work. I simply have no sympathy when it is realised that a horrible job has been done. The real world works like that, it is harsh and brutal, we make mistakes and we recover.

I think there is this thing called "Darwin's Theory of Evolution" that you can learn a lot about in university. It goes something like this.

Life evolved through a natural process of random mutations and natural selection.

Sounds to me like we are living it in the real world whereby matter interacting with matter can create anything and that random mutations and natural selection will dictate the outcome. Those that have followed best practice will end up higher in the chain than those that did not. A direct result of this random mutation called a vulnerability that turned into a worm that made us realise that we have to evolve just a little bit more.

>
>
>> * *How many of the systems vulnerable internally are protected with an IDS? (slim to none?)*
>>
>
> *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.

>
>
>> * *How many of the systems vulnerable from the internet are implemented and administered by an MCSE or equivalent? (nearly all?)*
>>
>
> *Funny, the only MCSE we've ever had left years ago. AFAIK we don't have a single person on staff with acronyms after their name. We do have an excellent Windows admin who used to be Banyan Vines certified. Usually, if a person gets acronyms, they leave for greener pastures.*
>
>
>> * *I am still a firm believer in the ability of the human race to learn by making mistakes. (it can be fun)*
>>
>
> *Please come to UTD next week. You can participate in the "fun".*
>

I appreciate the offer to join you but I think I may be busy with my own fun.

Full-Disclosure – We believe in it.

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

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