

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

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-07/1007.html>

From: Chris Paget (chrisp_at_ngssoftware.com)

Date: 07/27/03

To: Jason <security@brvenik.com>

Date: Sun, 27 Jul 2003 01:11:45 -0400 (Eastern Daylight Time)

Comments inline.

On Sun, 27 Jul 2003, Jason wrote:

> *The war begins...*

I hope so. Discussion of the hows and why's and morals of security and disclosure is **always** a good thing – which was partly why I made the original post.

> *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.*

In an ideal world, everyone would be patched by now. The problem is, this is not an ideal world, most people will still be unpatched. As for best practices – have you ever tried disabling RPC? It's not actually possible – in fact, WinXP and 2003 will automatically reboot if RPC stops. As for DCOM – the setting to disable it is a suggestion only, and applications can and will re-enable it whenever they use it, or else they'll just plain break. So which "best practices" are you talking about? Are you planning to install a separate firewall for every machine? If so, maybe I should buy some stock in Zone Labs or ISS...!

> > *Scanners are good; I agree they give out more information than an advisory, but it's still a step away from giving the kiddies a tool. Those in the know will always be able to write an exploit from minimal details; whether or not the pre-pubescent h4xx0rs get hold of it is another matter though.*

>

> *I would rather have a pre-pubescent cracker knocking on the door with a published sploit that I was forced to patch against any day when compared to the 1337 h4x0r w17h 4 g04l and the funding to achieve it.*

But you'd still patch either way, right? So we're talking about the difference between a knowledgeable, determined attacker (who can never be kept out) and a

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

skript kiddie with a tool, who is just an annoyance. But because of the exploit code, he's now a skript kiddie with a ten-thousand-node DDoS network at his disposal, who can (and probably will) DDoS anyone, anywhere, and there's nothing you can do to prevent it (short of getting very friendly with your upstream provider).

> *** Far too many people wait to patch until there is "published" exploit code. ***

I agree – there's far too many people who wait. But what about all the millions of home users who don't even know what a security patch *IS*, let alone how to find them? Most people buy a computer, stick it on the net, and expect it to work. They don't expect to be downloading updates every week.

> *** If you have assets worth protecting you hire people who are capable of protecting them. ***

The organisation concerned has hired many people who are perfectly capable of protecting their assets. The problem is, they're concerned about the business as well – and given Microsoft's track history with patches, I can understand their not wanting to install every patch on every mission-critical server the moment it is released. Allowing people to work is the primary goal of every server; security HAS to come second to that.

> ** How many of the systems in your typical multinational organization require the use of DCOM? (slim to none?)*

Agreed – very few, if any.

> ** How many of the systems that require DCOM need rpc exposed to everyone? (slim to none?)*

Also agreed. But how many organisations firewall off internal servers from internal users (slim to none). Bad practice, I'll agree, but expensive to implement if you choose to do it.

> ** How many of the systems exposed to everyone have weak administrative passwords? (nearly all?)*

Define "weak". If you mean "guessable within a week", I'd expect it to be very few. If you mean "crackable from a copy of the SAM by an attacker with average resources before the password expires", probably most – especially given the recent advances in hash chaining techniques.

> ** How many of the systems vulnerable internally would have been protected by an IPS if it had a way of protecting? (slim to none?)*

>

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

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

Detection and prevention is easier than you might think. The moment that an IDS detects the string "Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Corp." in a network packet, it's a fair bet that it's as the result of an exploit. Block the connection, block the IP.

As for how many are protected – not enough, which is again a cost issue. You ever looked at the price of an ISS RealSecure sensor? And then multiplied that by a thousand to cover all your servers? Besides – how many system administrators have the time to watch the IDS given the number of patches they have to install on all their servers?

- > ** How many of the systems vulnerable from the internet are implemented*
- > *and administered by an MCSE or equivalent? (nearly all?)*

Agreed. But I think many people on this list would agree that an exam you can pass after reading a book the night before is not worth much.

- > ** I am still a firm believer in the ability of the human race to learn*
- > *by making mistakes. (it can be fun)*

You and me both. But how many worms is it going to take?

- > ** I like beer! 1 l0v3 s3x!*

Amen.

- > ** These are my opinions and not those of my employer.*

Also amen.

Chris

Full-Disclosure – We believe in it.

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