

Re: DCOM Security.

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-09/0427.html>

From: n0g0o13 (ttw_at_cobbled.net)

Date: 09/28/05

Date: Wed, 28 Sep 2005 21:46:12 +0100

To: njfanelli@hotmail.com

On 26.09-16:54, njfanelli@hotmail.com wrote:

- > *I'm unfamiliar with Microsofts component services.*
- > *A client of mine has a local workgroup application that creates a*
- > *connection (ipsec) to a domain server, the application calls a*
- > *server component (dcom) via anonymous access. The developer has a*
- > *password embedded with in the local app to authenticate the*
- > *anonymous account. From this point the component forwards over a*
- > *request to another server for a Foxpro database (without any*
- > *additional security). Is there a way to exploit the anonymous*
- > *account if the workgroup client were to get compromised? How*
- > *concerned should I be with the possibility of the code being*
- > *decompiled? Additionally the programmer has domain credentials hard*
- > *coded into the application in order to perform an upload of*
- > *information that is created. Suggestions? Thank you in advance*

DCOM is nothing to do with security it is the distributed object model — microsoft's version of CORBA — if you will. i'm not an expert but there is basically no security offered by DCOM.

this sounds like typical braindamage programming and security being patched over with whatever could be found.

you'll have trouble getting the password or domain info from the wire as it's going to be encrypted but the chances are that

if you can get a copy of the binary you could de-compile it but i don't think that will be necessary. a simple dump of it will likely yeild results (remember unicode, though).

you have two challenges. cracking the workstation to get the binary from which to extract username, password, and domain info. this will not be much if you can gain physical access to the computer as a simple floppy or memory stick will do the job perfectly.

the second challenge is going to be accessing the server. if you are lucky then the server is only using IPSEC to hide the fact that

SecurityFocus Penetration: Re: DCOM Security.

the password is plain text (which is highly probable). this means you can use an open connection from anywhere else and crack away at both the DCOM connection object and possibly the foxpro DB (which is probably simpler). if it's not -- if there's a reasonable policy on the server connections -- then you have to crack that somehow. if you can gain privileged access to the workstation then you are set -- review and copy the policy and any keys/passwords required.

this probably isn't going to be a hard one to crack.

good luck with it.

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do! Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831
