HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza ranjivosti u RPC DCOM komponenti Windows operacijskih sustava

CCERT-PUBDOC-2003-07-30

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

RPC (engl. *Remote Procedure Call*) je protokol koji osigurava mehanizme potrebne za komunikaciju među procesima koji se ovijaju na lokalnom i udaljenom računalu. Na taj je način program na lokalnom računalu u mogućnosti transparentno izvoditi programski kod na udaljenom računalu.
16.07.2003. LSD (*Last Stage of Delirium*) grupa objavila je postojanje sigurnosnog propusta u Microsoftovoj implementaciji RPC protokola. Ova ranjivost obuhvaća gotovo sve inačice Microsoft Windows operacijskog sustava, uključujući i Microsoft Windows Server 2003. Postojanje sigurnosnog propusta potvrdio je i Microsoft, koji je već objavio sigurnosne zakrpe koje rješavaju spomenuti problem.

2. Analiza ranjivosti

Ranjivost je pronađena unutar dijela implementacije RPC protokola koji je zadužen za razmjenu poruka putem TCP/IP protokola i izravno se odražava na rad DCOM (engl. *Distributed Component Object Model*) sučelja koje omogućuje komunikaciju između programa na udaljenim računalima. Zbog nedostatne provjere ispravnosti poruka koje se razmjenjuju, moguće je uzrokovati napad prepisivanjem podataka na stogu.
Slanjem pažljivo oblikovane poruke na port 135 ranjivog računala, napadač je u mogućnosti izvršiti proizvoljan programski kôd pod ovlastima administratora sustava.
Budući da je RPC sučelje integralni dio svih modernih Windows operacijskih sustava, ovim propustom pogođeni su Windows NT 4.0, Windows 2000, Windows XP i Windows Server 2003 operacijski sustavi, bez obzira na instalirane sigurnosne zakrpe.

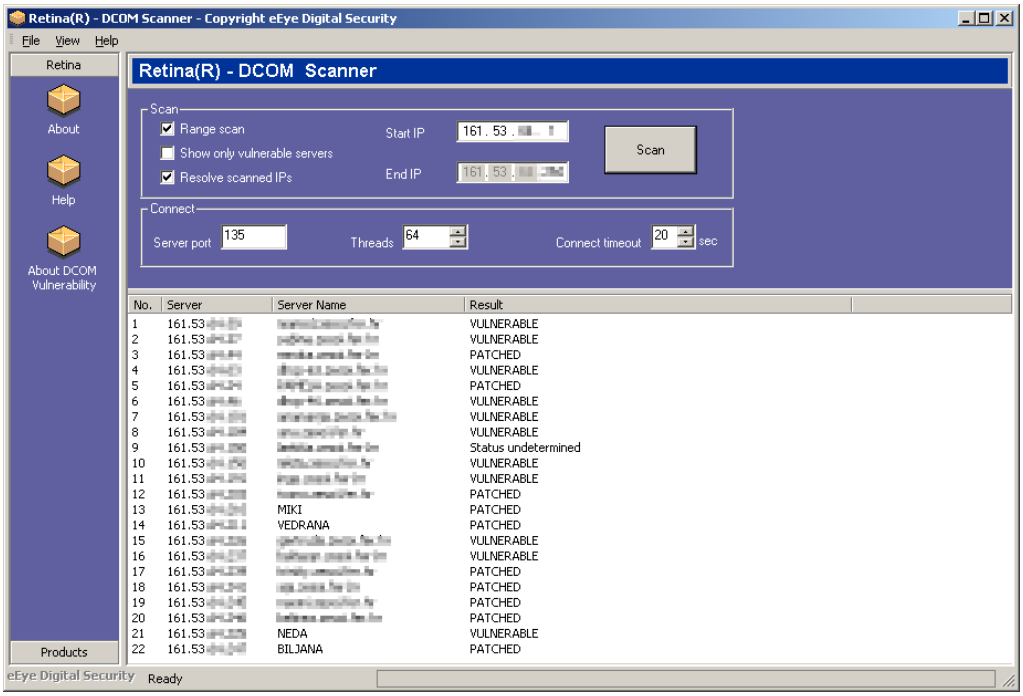
3. Detektiranje i uklanjanje ranjivosti

3.1. Detektiranje osjetljivih računala

U svrhu lakšeg detektiranja računala osjetljivih na opisani propust, tvrtke ISS (*Internet Security Systems*) i eEye Digital Security izdale su jednostavne alate koji pregledavaju mrežu u potrazi za ranjivim računalima. Korištenje ovih alata administratorima velikih računalnih mreža olakšava pronalaženje ranjivih računala.

3.1.1. eEye Retina RPC DCOM Scanner

Retina programski paket komercijalni je alat za pregledavanje i identifikaciju sigurnosnih nedostataka unutar računalnih sustava. Program omogućuje automatizirano pregledavanje većeg broja računala u svrhu uočavanja potencijalnih sigurnosnih nedostataka koji u sustav unose sigurnosni rizik. Na temelju rezultata dobivenih pokretanjem Retina programskog paketa moguće je poduzeti odgovarajuće zaštitne mjere koje će ukloniti identificirane propuste a samim time i podići sigurnosni nivo sustava.
Tvrtka eEye odlučila je korisnicima ponuditi besplatnu inačicu Retina alata koja je ograničena isključivo na pretraživanje propusta u Microsoftovoj implementaciji RPC protokola. Na slici 1 prikazano je sučelje Retina RPC DCOM alata.



Slika 1: Sučelje Retina RPC DCOM alata

Dvostrukim klikom miša na IP adresu računala koje je označeno kao ranjivo, korisniku se prikazuju kratke upute za uklanjanje ranjivosti. Ovaj alat moguće je dohvatiti sa adrese http://www.eeye.com/html/Research/Tools/Download.asp?file=RetinaRPCDCOM.

3.1.2. ISS scanms.exe Scanner

Scanms.exe je jednostavan alat koji se pokreće u naredbenom retku i pregledava zadani raspon IP adresa. Scnams koristi potpuno neprimjetne metode pregledavanja, tj. ne pokušava iskoristiti ranjivost niti se spojiti na računalo i provjeriti da li je instalirana odgovarajuća zakrpa. Budući da rezultati ovakvog pregledavanja nisu u potpunosti pouzdani, koriste se dvije različite metode kako bi se izbjegla mogućnost pogreške.
Primjer upotrebe scanms alata izgleda ovako:

```
D:\>scanms 192.168.0.1-192.168.0.254
--- ScanMs Tool --- (c) 2003 Internet Security Systems ---
 Scans for systems vulnerable to MS03-026 vuln
 More accurate for WinXP/Win2k, less accurate for WinNT
 ISS provides no warrantees for any purpose
 Use at own risk. Runs best from WinXP.
IP Address               REMACT   SYSACT   DCOM Version
-----------------------------------------------------
192.168.0.246            [ptch]   [ptch]   5.6
192.168.0.44             [....]   [ptch]   0.0
192.168.0.247            [....]   [ptch]   0.0
192.168.0.67             [....]   [VULN]   0.0
192.168.0.58             [ptch]   [....]   5.6
192.168.0.160            [ptch]   [ptch]   5.6
192.168.0.32             [ptch]   [ptch]   5.6
192.168.0.180            [ptch]   [ptch]   5.6
192.168.0.211            [ptch]   [....]   5.6
192.168.0.24             [ptch]   [ptch]   5.6
192.168.0.225            [ptch]   [ptch]   5.6
192.168.0.237            [ptch]   [ptch]   5.6
192.168.0.206            [ptch]   [ptch]   5.6
```

```
D:\>
```

Iz primjera je vidljivo da je računalo na IP adresi 192.168.0.67 detektirano kao ranjivo. Stupci REMACT i SYSACT predstavljaju rezultate dobivene svakom od pojedinih metoda pregledavanja. Računala koje ne osluškuju mrežni promet na portu 135 neće se testirati i neće biti prikazana u ispisu.
Ovaj jednostavan alat nalazi se na adresi http://www.iss.net/support/product_utilities/ms03-026rpc.php.

3.2. Uklanjanje ranjivosti

3.2.1. Instalacija zakrpe

Za uklanjanje ovog sigurnosnog propusta Microsoft preporučuje hitnu instalaciju zakrpe pod rednim brojem MS03-026.
Budući da će zakrpa za ovaj propust biti uključena tek u buduće Microsoft *service pack-ove* (Windows 2000 SP5, Windows XP SP2 i Windows Server 2003 SP1), potrebno ju je instalirati pomoću Windows Update-a ili ručno dohvatiti binarnu datoteku koja sadrži zakrpu. Na stranici http://support.microsoft.com/?kbid=823980 nalaze se detaljne upute za instalaciju zakrpi, kao i same zakrpe za pojedine inačice Microsoft Windows operacijskog sustava. Dohvaćenu .exe datoteku, najjednostavnije je ručno pokrenuti nakon čega se otvara prozor za instalaciju zakrpe (*Slika 2*).

Slika 2: Sučelje za instalaciju zakrpe MS03-036

Ukoliko je zakrpa ispravno instalirana, u Windows Registry-u trebali bi se pojaviti sljedeći ključevi:

Operacijski ustav	Ključ
Windows NT 4.0	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Hotfix\Q823980
Windows 2000	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB823980
Windows XP Gold	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP1\KB823980
Windows XP SP 1	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP2\KB823980
Windows Server 2003	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP1\KB823980

3.2.2. Alternativne metode uklanjanja ranjivosti

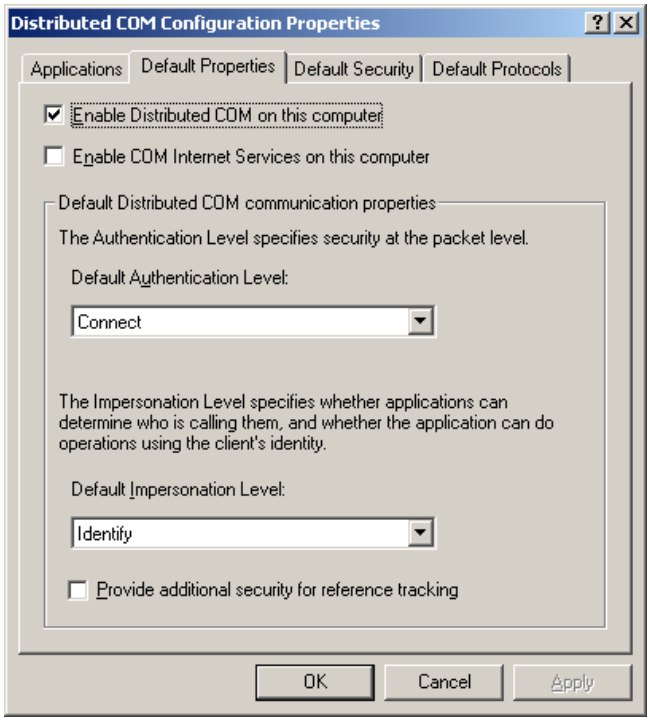
Iako je instalacija zakrpe najbolje i jedino u potpunosti sigurno rješenje, rizik od ranjavanja računala može se ukloniti i nekom od alternativnih metoda. Naravno, metode koje će biti opisane u nastavku treba smatrati isključivo kao privremeno rješenje i primijeniti ih isključivo u nedostatku odgovarajućih zakrpi ili kao dodatnu mjeru zaštite.

Najjednostavniji oblik zaštite internih računalnih mreža je filtriranje TCP i UDP portova broj 135 na vatrozidu. Na ovaj način onemogućeno je uspostavljanje RPC komunikacijske veze računalima koja se nalaze izvan mreže zaštićene vatrozidom. Osim porta 135 poželjno je na vatrozidu filtrirati i TCP/UDP portove 139 i 445, kao i sve ostale portove na kojima se nalaze servisi koji koriste RPC protokol. Ovom metodom, mreža nije zaštićena od malicioznih korisnika koji posjeduju pristup lokalnim računalima.

Korisnici Windows XP i Windows Server 2003 operacijskih sustava filtriranje portova preko kojih se odvija RPC komunikacija mogu filtrirati i lokalno, na samom računalu, upotrebom *Internet Connection Firewall-a*. Inicijalne postavke *Internet Connection Firewall-a* blokiraju sav RPC promet prema računalu.

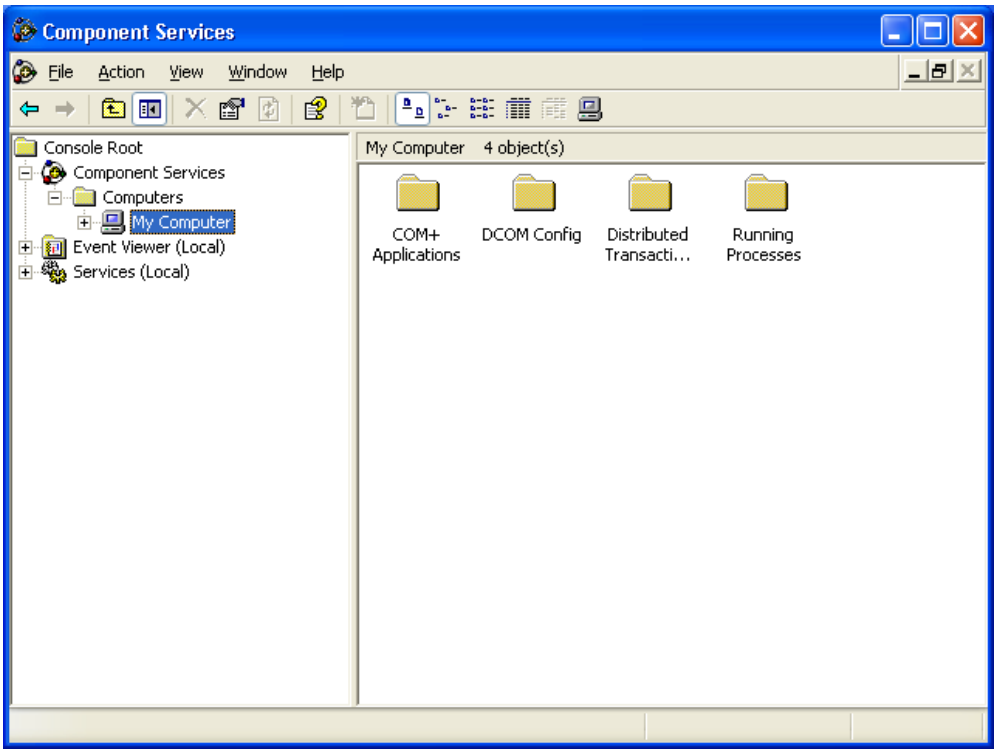
Računala se mogu zaštititi i onemogućavanjem RPC DCOM komunikacije, ali u tome slučaju sva interprocesna komunikacija sa takvim računalima biti će onemogućena. Za ponovno omogućavanje jednom isključene RPC DCOM komunikacije potreban je fizički pristup računalu.

Za onemogućavanje RPC DCOM komunikacije na Windows 2000 računalima potrebno je pokrenuti naredbu `dcomcnfg.exe`, nakon čega se pojavljuje prozor za podešavanje DCOM postavki (*Slika 3*). Unutar *Default properties* sekcije potrebno je isključiti opciju "*Enable Distributed COM on this Computer*" i kliknuti mišem na OK.



Slika 3: Podešavanje DCOM postavki

Korisnicima Windows XP i Windows Server 2003 operacijskih sustava, nakon pokretanja `dcomcnfg.exe` naredbe, otvara se *Component Services* prozor (*Slika 4*).



Slika 4: Podešavanje DCOM postavki na Windows XP i Windows Server 2003 računalima

Unutar prozora potrebno je odabrati stablo *Computers*, koje se nalazi pod sekcijom *Component Services*. Desni klik mišem na odabrano računalo (npr. *My Computer* za lokalno računalo) otvoriti će padajući izbornik u kojem je potrebno odabrati "*Properties*". Ostatak postupka identičan je onome za Windows 2000 računala.

4. Zaključak

Ovaj sigurnosni propust predstavlja prijetnju vrlo visokog rizika i svim korisnicima Windows operacijskih sustava preporuča se hitna primjena službeno izdanih zakrpi. Programski kôd koji iskorištava opisanu ranjivost i malicioznom korisniku omogućuje pristup naredbenom retku kompromitiranog računala dostupan je na Internetu što dodatno povećava rizik kompromitiranja sustava.