HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Qchain programskog paketa

CCERT-PUBDOC-2003-02-04

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

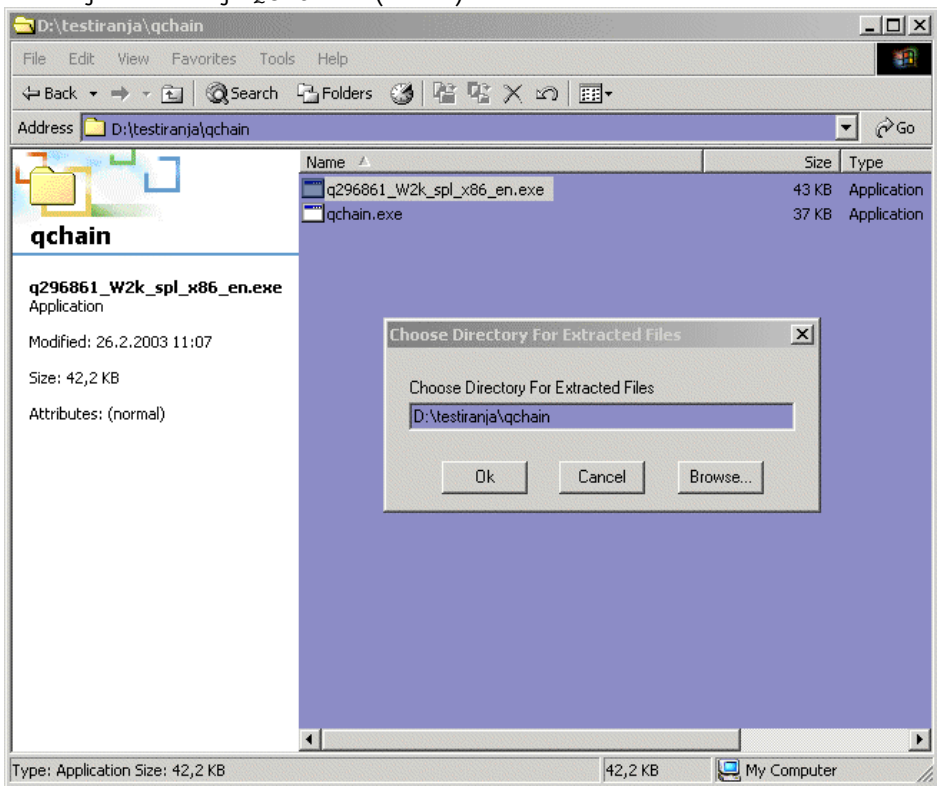
Microsoft je objavio alat pod imenom `Qchain` koji administratorima sustava daje mogućnost instalacije više zakrpi odjednom, bez potrebe za restartanjem računala između instalacija. Pomoću ovog programa olakšava se instalacija Windows operacijskih sustava i njihovo daljnje održavanje. Ovaj alat se može koristiti na sljedećim operacijskim sustavima:

- Microsoft Windows NT Server, Enterprise Edition 4.0,
- Microsoft Windows NT Server 4.0 Terminal Server Edition,
- Microsoft Windows NT Server 4.0,
- Microsoft Windows NT Workstation 4.0,
- Microsoft Windows 2000 Datacenter Server,
- Microsoft Windows 2000 Advanced Server,
- Microsoft Windows 2000 Professional,
- Microsoft Windows 2000 Server.

Potrebno je napomenuti da sustavi Windows XP i Windows 2000 sa instaliranim *Service Pack* 3 paketom imaju uključenu podršku za višestruku instalaciju zakrpi, tako da kod njih ne postoji potreba za korištenjem `Qchain` alata.

2. Instalacija i pokretanje Qchain-a

Posljednja inačica QChain programa nalazi se na adresi http://www.microsoft.com/downloads/release.asp?ReleaseID=29821. Alat se instalira pokretanjem instalacijske datoteke `q296861_W2k_spl_x86_en.exe` koja će otvoriti prozor u kojem se bira ciljani direktorij za instalaciju `Qchain`-a (Slika 1).



Slika 1: *Instalacija QChain-a*

Rezultat instalacije je naredba `qchain.exe` koja se pokreće iz naredbenog retka. Program kao parametar može primiti ime log datoteke u koju će se spremati podaci o radu. Ime log datoteke je dovoljno navesti prilikom pokretanja naredbe `Qchain`:

```
D:\qchain>qchain log_datoteka
```

3. Instalacija Windows zakrpi

Zakrpa je jedna (ili više) datoteka koje se koriste za ispravljanje grešaka u sustavu. Microsoft izdaje svoje zakrpe u obliku `.exe` datoteka koje se instaliraju jednostavnim pokretanjem. Instalacijski program za zakrpe prima sljedeće parametre:

- /F – zatvara sve aplikacije prije resetiranja računala,
- /N – ne radi uobičajeni backup izmijenjenih datoteka,
- /Z – onemogućuje restart računala nakon instalacije zakrpi,
- /Q – uključuje *quiet* način rada (nema interakcije s korisnikom),
- /M - koristi *unattended Setup* način rada za Windows 2000 sustav,
- /U - koristi *unattended Setup* način rada za Windows XP sustav,
- /L – ispisuje listu instaliranih zakrpi.

Batch datoteka koja bi instalirala više zakrpi odjednom izgledala bi ovako:

```
@echo off
setlocal
set PATHTOFIXES=E:\hotfix

%PATHTOFIXES%\Q123456_w2k_sp4_x86.exe /Z /M
%PATHTOFIXES%\Q123321_w2k_sp4_x86.exe /Z /M
%PATHTOFIXES%\Q123789_w2k_sp4_x86.exe /Z /M
```

4. Korištenje Qchain programa prilikom instalacije zakrpi

Prilikom instalacije zakrpi, određene datoteke nije moguće zamijeniti odmah već se nove datoteke smještaju u *Pending File Rename* red. Prilikom sljedećeg pokretanja računala, čita se sadržaj *Pending File Rename* reda i mijenjaju potrebne datoteke. U slučaju instalacije više zakrpi odjednom, bez restarta računala između svake od instalacija, javlja se sljedeći problem:

- Obje zakrpe sadrže *update* iste datoteke,
- Zakrpa A sadrži inačicu 3 navedene datoteke, dok zakrpa B sadrži inačicu 2 iste datoteke,
- Prilikom instalacije zakrpe A inačica 3 nove datoteke smješta se u *Pending File Rename red*,
- Prilikom instalacije zakrpe B inačica 2 iste datoteke smješta se u *Pending File Rename red*,
- Nakon restarta računala, instalirati će se inačica 2 nove datoteke zbog toga što je zadnja u redu.

Opisani scenarij rezultirao je instalacijom starije inačice zakrpane datoteke, što naravno nije poželjno. Zadatak `Qchain` alata je preuređivanje *Pending File Rename* reda tako da u njemu ostanu samo najnovije inačice datoteka koje se trebaju zamijeniti. `Qchain` se primjenjuje na sljedeći način:

- Instalaciju zakrpe potrebno je pokrenuti sa –Z parametrom koji sprječava restart računala nakon instalacije zakrpe. Uz korištenje –Z parametra preporučuje se korištenje i –Q parametra (engl. *quiet mode*) koji uklanja suvišne poruke koje se prikazuju u naredbenom retku.
- Nakon instalacije svih zakrpi pokreće se `Qchain` alat koji provjerava *Pending File Rename* red i iz njega uklanja starije inačice zakrpanih datoteka.
- Poslije instalacije svih zakrpi i pokretanja `QChain`-a, potrebno je resetirati računalo.

U svrhu lakše instalacije poželjno je napraviti *batch* datoteku koje će automatizirati proces instalacije. Primjer takve datoteke dan je u nastavku:

```
@echo off
setlocal
set PATHTOFIXES=some path
%PATHTOFIXES%\Q123456_w2k_sp2_x86.exe /Z /Q
%PATHTOFIXES%\Q123321_w2k_sp2_x86.exe /Z /Q
%PATHTOFIXES%\Q123789_w2k_sp2_x86.exe /Z /Q
%PATHTOFIXES%\qchain.exe
```

Kao što je već spomenuto, Qchain kao parametar prihvaća ime log datoteke u koju se spremaju snimke *Pending File Rename Operations* ključa koji se nalazi u Windows *Registry*-u, prije i poslije pokretanja Qchain-a. U nastavku je dan primjer log datoteke koji je rezultat instalacije tri zakrpe koje sadrže istu datoteku.

```
---- Old Information In The Registry ------
Source:C:\WINNT\inf\acpi.inf
Version: 5.0.2183.1
Destination:d:\ntsust\testregchech\1394.inf
Version: 5.0.2183.1

Source:C:\WINNT\inf\adm_mult.inf
Version: 5.0.2184.1
Destination:d:\ntsust\testregchech\1394.inf
Version: 5.0.2183.1

Source:C:\WINNT\inf\banshee.inf
Version: 5.0.2080.1
Destination:d:\ntsust\testregchech\1394.inf
Version: 5.0.2183.1

---- New Information In The Registry ------
Source:C:\WINNT\inf\adm_mult.inf
Version: 5.0.2184.1
Destination:d:\ntsust\testregchech\1394.inf
Version: 5.0.2183.1
```

Iz primjera *log* datoteke vidljivo je da su uklonjena dva zapisa koja su sadržavala starije inačice datoteke koja se treba instalirati i da je ostavljena samo najnovija inačica datoteke.

5. Ograničenja Qchain programa

Iako Qchain radi ispravno s većinom Windows NT 4.0 i Windows 2000 zakrpi, mogući su problemi sa zakrpama koje sadrže binarne datoteke navedene u Windows *Registry* ključu **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\KnownDLLs**.

Navedene binarne datoteke učitavaju se u memoriju prilikom pokretanja sustava. Pozivanjem GetFileVersionInfo funkcije, dobiti će se podaci o datoteci koja je učitana u memoriju, a ne o datoteci koja je prisutna na stvarnoj lokaciji na disku.

Budući da je KnownDLLs parametar učitan u radnu memoriju prilikom pokretanja sustava, instalacijski program za zakrpu mora zamijeniti ciljanu datoteku prije restarta računala zbog čega se neće kreirati zapis u *Pending File Rename* redu. Umjesto toga instalacijski program sklanja binarnu datoteku na privremenu lokaciju i umjesto nje instalira novu datoteku kreirajući pri tome *Pending File Rename* zapis koji će prilikom ponovnog podizanja sustava obrisati staru datoteku.

Qchain se obazire samo na one operacije koje izvode zamjenu binarnih datoteka i ignorira operacije koje brišu datoteke.

Sve Windows NT 4.0 i Windows 2000 (ranije od *Service Pack*-a 2) koriste GetFileVersionInfo metodu identifikacije paketa. U slučaju instalacije nekoliko Windows NT 4.0 zakrpi ili Windows 2000 zakrpi, koje su izdane ranije od *Service Pack*-a 2, koje sadrže preklapajuće KnownDLLs podatke ne postoji garancija da će Qchain instalirati posljednje inačice zakrpi za pojedine pakete.

Sljedeći primjer objašnjava navedeni problem:

- Instaliraju se dvije zakrpe A i B bez restarta računala između instalacija.
- Oba paketa sadrže Kernel32.dll datoteku koja se nalazi u KnownDLLs listi. Zakrpa A sadrži inačicu 3, zakrpa B inačicu 2, a na računalu je instalirana inačica 1 navedene datoteke.
- Prilikom instalacije zakrpe A, GetFileVersionInfo prijavljuje da je na računalu instalirana inačica 1 Kernel32.dll paketa. Budući da zakrpa sadrži noviju inačicu

datoteke, ona se kopira na odgovarajuće mjesto na disku. Stara inačica datoteke smješta se na privremenu lokaciju i kreira se *Pending File Rename* operacija koja će obrisati datoteku prilikom sljedećeg pokretanja računala.

- Kod instalacije zakrpe B, `GetFileVersionInfo` ponovo će prijaviti da je na računalu instalirana inačica 1 datoteke `Kernel32.dll`. Razlog tome je taj što se informacija o inačici čita iz datoteke `Kernel32.dll` koja se nalazi u memoriji, a ne iz one datoteke koja je instalirana na disku. Budući da je prijavljena inačica 1, pokrenuti će se instalacija inačice 2 kao i u prethodnom koraku.
- Kada se nakon instalacije zakrpi pokrene `Qchain` on će ignorirati *Pending File Rename* operacije koje brišu datoteke tj. neće učiniti ništa.
- Budući da je zakrpa B instalirana posljednja, prilikom ponovnog pokretanja računala u memoriju će se učitati inačica 2 datoteke `Kernel32.dll`, a *Pending File Rename* operacija će obrisati inačice 1 i 3.

Kao što se vidi iz primjera, unatoč korištenju `Qchain` alata, doći će do greške prilikom instalacije i neće se instalirati posljednja inačica zakrpane datoteke.

Gornji primjer ne odnosi se na zakrpe izdane nakon objavljivanja Windows 2000 *Service Pack* 2 paketa. Navedene zakrpe ispravljene su tako da `GetFileVersionInfo` ne pozivaju za datoteku učitanu u memoriju već za onu koja se nalazi na stvarnom mjestu na disku. Zbog toga je sve novije zakrpe moguće instalirati pomoću `Qchain` alata.

6. Zaključak

`Qchain` je vrlo koristan alat koji administratorima omogućuje lakšu i bržu instalaciju velikog broja zakrpi odjednom. Korisnost ovog programa naročito dolazi do izražaja kod velikog broja računala, jer se broj njihovog ponovnog pokretanja višestruko smanjuje.