Subject: Numerous segmentation faults on VE start
Posted by sgwestrip on Tue, 23 Oct 2007 21:15:25 GMT
View Forum Message <> Reply to Message

I am getting these errors when I try to start this VE. I can enter the VE but the network has not started. I have done a vzcfgvalidate and all seems OK there and I am now completely out of ideas. This is the first VE that has ever caused me any persistent problems. Any help would be gratefully received.

```
[root@virtual2 ~]# vzctl start 211
Starting VE ...
VE is mounted
Adding IP address(es): 10.0.0.101
bash: line 360: 19791 Segmentation fault      mkdir -p ${IFCFG_DIR}
bash: line 291: 19792 Segmentation fault      grep -qE '191.255.255.[0-1]' $file
bash: line 360: 19793 Segmentation fault      grep -q "${FAKEGATEWAYNET}/24 dev
${VENET_DEV}" ${ROUTE} 2>/dev/null
bash: line 61: 19794 Segmentation fault      grep -E "^$name=.*" $file >/dev/null 2>&1
bash: line 61: 19795 Segmentation fault      grep -E "^$name=.*" $file >/dev/null 2>&1
bash: line 344: 19796 Segmentation fault      grep -q 'if \[ "\${DEVICE}" = "lo" \]; then' ${file}
2>/dev/null
bash: line 458: 19798 Segmentation fault      mkdir -p ${IFCFG_DIR}/bak
Execution timeout expired
Got signal 15
Setting CPU units: 50788
Configure meminfo: 620921
Set hostname: sane.m4.net
bash: line 330: 19829 Segmentation fault      grep -q -E "[[:space:]]${val}" ${cfgfile} 2>/dev/null
bash: line 330: 19830 Done                    echo "${val}"
    19831 Segmentation fault      | grep "\." >/dev/null 2>&1
bash: line 152: 19832 Segmentation fault      grep -E "^\<$name\>" $file >/dev/null 2>&1
bash: line 61: 19833 Segmentation fault      grep -E "^$name=.*" $file >/dev/null 2>&1
File resolv.conf was modified
VE start in progress...
```

Many thanks,
Stephen Westrip

Subject: Re: Numerous segmentation faults on VE start
Posted by rickb on Wed, 24 Oct 2007 06:39:03 GMT
View Forum Message <> Reply to Message

When I see this, the VE has been compromised and a rootkit yielding non runnable binaries are instaled. check binary md5's against your latest backup and/or template.

Subject: Re: Numerous segmentation faults on VE start
Posted by sgwestrip on Wed, 24 Oct 2007 16:08:50 GMT
View Forum Message <> Reply to Message

Thank you for your reply.

It seems as though this VE was compromised with a rootkit named 'Whatis' and had changed 20 or so binaries in /bin. What is more alarming is that from the VE it had managed to changed the same binaries in /bin on the hardware node. I was surprised that this was even possible from the VE.

Anyway, it is all sorted out now. Thanks for pointing me in the right direction.

Stephen Westrip

Subject: Re: Numerous segmentation faults on VE start
Posted by dev on Wed, 24 Oct 2007 16:40:07 GMT
View Forum Message <> Reply to Message

it is almost impossible to get out of the VE chroot, so most likely you were simply hacked twice in VE and HN.

BTW, recently there was a severe x8664 kernel flaw, it could be used to hack you. So don't forget to upgrade kernel.