

## Re: Nessus against Novell file servers.

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-03/0079.html>

---

**From:** Barrie Dempster ([barrie\\_at\\_reboot-robot.net](mailto:barrie_at_reboot-robot.net))

**Date:** 03/16/05

Date: Wed, 16 Mar 2005 19:32:24 +0000

To: Roni Bachar <[roni@avnet.co.il](mailto:roni@avnet.co.il)>

Roni Bachar wrote:

<snip>

>

> *so test if this is your case if yes disable the ftp module.*

>

Good idea, until you consider that this is the pen-test mailing list frequented by pen-testers who should really be investigating this vulnerability to find out if it is a reproducible and therefore reportable DoS vulnerability. Going even further there may be exploitability.

I realise that the present situation is a VA only, so the client might not want this reported/exploited, but the OP should really investigate further. I don't believe it's common practice (at least I don't do it) to ignore a vulnerability because someone else hasn't released an exploit for it.

"disable the ftp module" is probably the most crazy statement I've seen this week (actually it's not but I just said that for effect).

My advice would be, disable the FTP module in order to continue your test, report the DoS as part of the pen-test report (if the client is interested to that extent) and then investigate further and disclose the vulnerability in whatever way your disclosure ethics define.

Don't switch it off and ignore it, \*please\*!!

--

With Regards..

Barrie Dempster (zeedo) - Fortiter et Strenue

blog: <http://zeedo.blogspot.com>

site: <http://www.bsrf.org.uk>

CA: [www.cacert.org](http://www.cacert.org)

"He who hingeth aboot, getteth hee-haw" - Victor (Still Game)

---

SecurityFocus Penetration: Re: Nessus against Novell file servers.

- application/x-pkcs7-signature attachment: S/MIME Cryptographic Signature