

## compromised server

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-08/0221.html>

---

**From:** jahmon ([jahmon\\_at\\_jahmon.com](mailto:jahmon_at_jahmon.com))

**Date:** 08/28/03

Date: Thu, 28 Aug 2003 10:41:59 -0400

To: [freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org)

I have a server that has been compromised.

I'm running version 4.6.2

when I do

*>last*

this line comes up in the list.

shutdown ~ Thu Aug 28 05:22

That was the time the server went down.

There seemed to be some configuration changes.

Some of the files seemed to revert back to default versions

(httpd.conf, resolv.conf)

Does anyone have a clue what type of exploit they may have used?

Is there anyway I can find out if there are any trojans installed?

Thanks

jahmon

---

[freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org) mailing list

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

To unsubscribe, send any mail to "[freebsd-security-unsubscribe@freebsd.org](mailto:freebsd-security-unsubscribe@freebsd.org)"