

## Re: [Corrected message] This OpenBSD local root hole may affect some FreeBSD systems

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2002-04/8928.html>

---

**From:** Borja Marcos ([borjamar@sarenet.es](mailto:borjamar@sarenet.es))

**Date:** 04/12/02

From: Borja Marcos <[borjamar@sarenet.es](mailto:borjamar@sarenet.es)>

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

Date: Fri, 12 Apr 2002 21:20:30 +0200

On Friday 12 April 2002 07:58, you wrote:

> *That's good to know! It looks as if NetBSD and Darwin have this feature*  
> *as well. But SunOS 5.8 doesn't (at least according to the docs at*  
> <http://www.freebsd.org/cgi/man.cgi?query=mail&apropos=0&sektion=0&manpath=S>  
> *unOS+5.8&format=html), so Solaris may be vulnerable.*

I have just tested Solaris 8 and it is not vulnerable. However, this is very old news. I reported a security hole in SCO Unix to CERT in 1993. I used this "feature" to modify root's crontab simply running a script which printed "~! commands" from "at".

An a security problem with reverse fingers and TCP Wrapper (see Wietse Venema's "Murphy's Laws and Computer Security") exploited exactly the same. As far as I know, that behavior was removed from mail programs; they only accept escape sequences (at least the ~!) when running from a terminal.

Borja.

To Unsubscribe: send mail to [majordomo@FreeBSD.org](mailto:majordomo@FreeBSD.org) with "unsubscribe freebsd-security" in the body of the message