

Re: possible compromise or just misreading logs

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-12/0025.html>

From: Dorin H (*bj93542_at_yahoo.com*)

Date: 12/08/03

Date: Mon, 8 Dec 2003 11:23:35 -0800 (PST)

To: Craig Riter <criter@riter.com>

Hi there,

About file integrity check (only one piece of the puzzle, but a necessary one):

Use aide (last tripwire is yet to be updated –do not compile–, see maintainer work).

To prevent the mentioned attacks, keep your hashes OFF your box. To compute/verify hashes, always boot from a secure live cd.

Downside: you have to do this at each update. To maintain the level of security, try something like:

1. boot secure cd
2. verify the hashes by comparing to the last version from the external source (use a log, better than override previous hashes).
3. If ok, do the update (have your sources downloaded locally before and verified; the FreeBSD online update system is yet to be secured: see list discussion)
[Paranoia: 4.boot again your safe cd and recompute & save the new hashes]
4. Recompute the new hashes and save them externally.

Add–on. You should do this offline to remove the window of opportunity in step 3, while updating the tracked files.

Hope this helps,
/Dorin.

PS. If you have a Web server, I'd rather start by add at least some kind of firewall and an external syslog before thinking of the file integrity check anyway.

- > *Second, what are people using for intrusion*
- > *detection? This is something I*
- > *have thought about but never really thought I*

FreeBSD-Security: Re: possible compromise or just misreading logs

> *needed until now.*

>

Do you Yahoo!?

Free Pop-Up Blocker – Get it now

<http://companion.yahoo.com/>

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"