-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

To the Free Software Community:

Summary

* gnuftp, the FTP server for the GNU project was root compromised.

* After substantial investigation, we don't believe that any GNU source has been compromised.

* To be extra-careful, we are verifying known, trusted secure checksums of all files before putting them back on the FTP site.

Events Concerning Cracking of Gnuftp

A root compromise and a Trojan horse were discovered on gnuftp.gnu.org, the FTP server of the GNU project. The machine appears to have been cracked in March 2003, but we only very recently discovered the crack. The modus operandi of the cracker shows that (s)he was interested primarily in using gnuftp to collect passwords and as a launching point to attack other machines. It appears that the machine was cracked using a ptrace exploit by a local user immediately after the exploit was posted on bugtraq.

(For the ptrace bug, a root-shell exploit was available on 17 March 2003, and a working fix was not available on linux-kernel until the following week. Evidence found on the machine indicates that gnuftp was cracked during that week.)

Given the nature of the compromise and the length of time the machine was compromised, we have spent the last few weeks verifying the integrity of the GNU source code stored on gnuftp. Most of this work is done, and the remaining work is primarily for files that were uploaded since early 2003, as our backups from that period could also theoretically be compromised.

Historical Integrity Checks

We have compared the md5sum of each source code file (such as .tar.gz, .tar.bz2, diff's, etc.) on ftp.gnu.org with a known good data. The file, ftp://ftp.gnu.org/before-2003-08-01.md5sums.asc, contains a list of files in the format:

MD5SUM FILE [REASON, ... REASON]

The REASONs are a list of reasons why we believe that md5sum is good for that file. The file as a whole is GPG-signed.

Remaining Files

The files that have not been checked are listed in the root directory as "MISSING-FILES". We are in the process of asking GNU maintainers for trusted secure checksums of those files before we put them in place.

We have lots of evidence now to believe that no source has been compromised -- including the MO of the cracker, the fact that every file we’ve checked so far isn’t compromised, and that searches for standard source trojans turned up nothing.

However, we don’t want to put files up until we’ve had a known good source confirm that the checksums are correct.

Alpha FTP Site

The Alpha FTP site at ftp://alpha.gnu.org/ has been a lower priority for us, but we plan to follow the same procedure there.

Moving Forward

All releases after the 2003-08-01 date will have checksums GPG-signed by the GNU maintainer who prepared the release, and unfortunately we’ll be discontinuing local shell access to the FTP server for GNU maintainers.

```
- --
Bradley M. Kuhn, Executive Director
Free Software Foundation     |  Phone: +1-617-542-5942
59 Temple Place, Suite 330   |  Fax:   +1-617-542-2652
Boston, MA 02111-1307  USA   |  Web:   http://www.gnu.org
```

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)

iD8DBQE/Oo2W53XjJNtBs4cRAj6aAJ9ZjHi+zUB0QQD/NzxdUn22oDBOZwCbBda3
d0a55Wg9HLKNFxz+DKCFaQA=
=4LJ3
-----END PGP SIGNATURE-----