

CERT Advisory CA-2003-21 GNU Project FTP Server Compromise

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2003-08/0004.html>

From: CERT Advisory (cert-advisory_at_cert.org)

Date: 08/13/03

Date: Wed, 13 Aug 2003 17:49:09 -0400

To: cert-advisory@cert.org

-----BEGIN PGP SIGNED MESSAGE-----

CERT Advisory CA-2003-21 GNU Project FTP Server Compromise

Original issue date: August 13, 2003

Last revised: --

Source: CERT/CC

A complete revision history is at the end of this file.

Overview

The CERT/CC has received a report that the system housing the primary FTP servers for the GNU software project was compromised.

I. Description

The GNU Project, principally sponsored by the Free Software Foundation (FSF), produces a variety of freely available software. The CERT/CC has learned that the system housing the primary FTP servers for the GNU software project, gnuftp.gnu.org, was root compromised by an intruder. The more common host names of ftp.gnu.org and alpha.gnu.org are aliases for the same compromised system. The compromise is reported to have occurred in March of 2003.

The FSF has released an announcement describing the incident.

Because this system serves as a centralized archive of popular software, the insertion of malicious code into the distributed software is a serious threat. As the above announcement indicates, however, no source code distributions are believed to have been maliciously modified at this time.

II. Impact

Cert: CERT Advisory CA-2003-21 GNU Project FTP Server Compromise

The potential exists for an intruder to have inserted back doors, Trojan horses, or other malicious code into the source code distributions of software housed on the compromised system.

III. Solution

We encourage sites using the GNU software obtained from the compromised system to verify the integrity of their distribution.

Sites that mirror the source code are encouraged to verify the integrity of their sources. We also encourage users to inspect any and all other software that may have been downloaded from the compromised site. Note that it is not always sufficient to rely on the timestamps or file sizes when trying to determine whether or not a copy of the file has been modified.

Verifying checksums

The FSF has produced PGP-signed lists of known-good MD5 hashes of the software packages housed on the compromised server. These lists can be found at

<ftp://ftp.gnu.org/before-2003-08-01.md5sums.asc>
<ftp://alpha.gnu.org/before-2003-08-01.md5sums.asc>

Note that both of these files and the announcement above are signed by Bradley Kuhn, Executive Director of the FSF, with the following PGP key:

```
pub 1024D/DB41B387 1999-12-09 Bradley M. Kuhn <bkuhn@fsf.org>
   Key fingerprint = 4F40 645E 46BE 0131 48F9 92F6 E775 E324 DB41 B387
uid Bradley M. Kuhn (bkuhn99) <bkuhn@ebb.org>
uid Bradley M. Kuhn <bkuhn@gnu.org>
sub 2048g/75CA9CB3 1999-12-09
```

The CERT/CC believes this key to be valid.

As a matter of good security practice, the CERT/CC encourages users to verify, whenever possible, the integrity of downloaded software. For more information, see IN-2001-06.

Appendix A. – Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Free Software Foundation

Cert: CERT Advisory CA-2003-21 GNU Project FTP Server Compromise

The current files on alpha.gnu.org and ftp.gnu.org as of 2003-08-02 have all been verified, and their md5sums and the reasons we believe the md5sums can be trusted are in:

<ftp://ftp.gnu.org/before-2003-08-01.md5sums.asc>
<ftp://alpha.gnu.org/before-2003-08-01.md5sums.asc>

We are updating that file and the site as we confirm good md5sums of additional files. It is theoretically possible that downloads between March 2003 and July 2003 might have been source-compromised, so we encourage everyone to re-download sources and compare with the current copies for files on the site.

Appendix B. References

- * FSF announcement regarding the incident –
<ftp://ftp.gnu.org/MISSING-FILES.README>
- * CERT Incident Note IN-2001-06 –
http://www.cert.org/incident_notes/IN-2001-06.html

The CERT/CC thanks Bradley Kuhn and Brett Smith of the Free Software Foundation for their timely assistance in this matter.

Feedback can be directed to the author: Chad Dougherty.

This document is available from:
<http://www.cert.org/advisories/CA-2003-21.html>

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

Cert: CERT Advisory CA-2003-21 GNU Project FTP Server Compromise

We strongly urge you to encrypt sensitive information sent by email.
Our public PGP key is available from
http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site
<http://www.cert.org/>

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

subscribe cert-advisory

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2002 Carnegie Mellon University.

Revision History

August 13, 2003: Initial release

-----BEGIN PGP SIGNATURE-----

Version: PGP 6.5.8

```
iQCVAwUBPzqwFWjtSoHZUTs5AQQN4AQAvL/u+S+FpkNWtBH/fe9DCLJQM21I/dzt
QPU0prMxTq53ntvTOAth+yFPtbceDaWuLHakju0mL4OSU0Fp+VsXbXnF5ypE+0r
S5mHpMxSmvPBPBNTIMQUGybEKK783P9Ty2lhXxawEW9JbdgMOY44clo2VIupgxuZ
OeyQrFbsq54=
=/72G
```

-----END PGP SIGNATURE-----