CERT Incident Note IN-2001-06: Verification of Downloaded Software

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Verification of Downloaded Software

Release Date: June 8, 2001

The CERT/CC has received reports and inquiries regarding the integrity of downloaded software.

Background

When downloading software from online repositories, it is important to consider the possibility that the site has been compromised. One of the threats that users face is that intruders could include malicious code in the software packages distributed by those sites. This code could take the form of Trojan horse programs or backdoors.

There are precautions that users can take when downloading software. There are also ways that software publishers and distributors can provide verification of the authenticity of their software.

Users

We strongly encourage users to verify cryptographic signatures (e.g. PGP) of all downloaded software. Cryptographic signatures provide reasonable assurance that the files have not been modified either on the server or in transit. They also allow for verification of the signer's identity.

In situations where cryptographic signatures are not provided but some other form of checksum (e.g. MD5 hash) has been included, we encourage users to verify the software against these checksums. Although checksums alone provide no information about when the checksum was generated or who generated it, they do provide some evidence that the files have not been modified. However, it is possible that an intruder could have replaced both the software and checksums. Therefore, when possible, we recommend that users compare the checksums provided by multiple sources, such as mirror sites.

If no signatures or checksums are provided, we recommend that users perform a thorough examination of all downloaded source code before compilation and installation. In the case of binaries where examination is difficult or impossible, users may wish to perform offline testing before installing downloaded binaries into production environments.

Software Publishers & Distributors

We encourage anyone publishing or distributing software to use cryptographic signatures and checksums. Publishers and distributors should generate the signatures and checksums on a non-public machine to reduce the risk of compromised private keys.

For more information

General information about Pretty Good Privacy (PGP), including some free software implementations, can be found at

http://www.pgpi.org/

The commercial version of PGP, from PGP Security, Inc., can be found at

http://www.pgp.com/

Information about GNU Privacy Guard, a freely available OpenPGP-compliant implementation, can be found at

http://www.gnupg.org/

Information on Trojan Horse programs can be found in the following document:

http://www.cert.org/advisories/CA-1999-02.html

Author(s): Chad Dougherty and Allen Householder