CERT Advisory CA-2002-24 Trojan Horse OpenSSH Distribution

Original issue date: August 1, 2002
Last revised: August 2, 2002
Source: CERT/CC

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

Overview

The CERT/CC has received confirmation that some copies of the source code for the OpenSSH package were modified by an intruder and contain a Trojan horse.

We strongly encourage sites which employ, redistribute, or mirror the OpenSSH package to immediately verify the integrity of their distribution.

I. Description

The CERT/CC has received confirmation that some copies of the source code for the OpenSSH package have been modified by an intruder and contain a Trojan horse. The following advisory has been released by the OpenSSH development team

> http://www.openssh.com/txt/trojan.adv

The following files were modified to include the malicious code:

> *openssh-3.4p1.tar.gz*
> *openssh-3.4.tgz*
> *openssh-3.2.2p1.tar.gz*

These files appear to have been placed on the FTP server which hosts ftp.openssh.com and ftp.openbsd.org on the 30th or 31st of July, 2002. The OpenSSH development team replaced the Trojan horse copies with the original, uncompromised versions at 13:00 UTC, August 1st, 2002. The Trojan horse copy of the source code was available long enough for copies to propagate to sites that mirror the OpenSSH site.

The Trojan horse versions of OpenSSH contain malicious code that is run when the software is compiled. This code connects to a fixed remote server on 6667/tcp. It can then open a shell running as the user who compiled OpenSSH.

II. Impact

An intruder operating from (or able to impersonate) the remote address specified in the malicious code can gain unauthorized remote access to any host which compiled a version of OpenSSH from this Trojan horse version of the source code. The level of access would be that of the user who compiled the source code.

III. Solution

We encourage sites who downloaded a copy of the OpenSSH distribution to verify the authenticity of their distribution, regardless of where it was obtained. Furthermore, we encourage users to inspect any and all software that may have been downloaded from the compromised site. Note that it is not sufficient to rely on the timestamps or sizes of the file when trying to determine whether or not you have a copy of the Trojan horse version.

Where to get OpenSSH

The primary distribution site for OpenSSH is

> http://www.openssh.com/

Sites that mirror the OpenSSH source code are encouraged to verify the integrity of their sources.

Verify MD5 checksums

You can use the following MD5 checksums to verify the integrity of your OpenSSH source code distribution:

Correct versions:

> *459c1d0262e939d6432f193c7a4ba8a8 openssh-3.4p1.tar.gz*
> *d5a956263287e7fd261528bb1962f24c openssh-3.4p1.tar.gz.sig*
> *39659226ff5b0d16d0290b21f67c46f2 openssh-3.4.tgz*
> *9d3e1e31e8d6cdbfa3036cb183aa4a01 openssh-3.2.2p1.tar.gz*
> *be4f9ed8da1735efd770dc8fa2bb808a openssh-3.2.2p1.tar.gz.sig*

At least one version of the modified Trojan horse distributions was reported to have the following checksum:

Trojan horse version:

> *3ac9bc346d736b4a51d676faa2a08a57 openssh-3.4p1.tar.gz*

Verify PGP signature

Additionally, distributions of the portable release of OpenSSH are distributed with detached PGP signatures. Note that the Trojan horse versions were not signed correctly, and attempts to verify the signatures would have failed.

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

http://www.cert.org/incident_notes/IN-2001-06.html

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.

Connectiva Linux

> *Conectiva Linux distributes openssh-3.4p1 as a security update. The distributed copy is the original one and is not affected by this trojan. The detached digital signature is always checked before building third party packages.*

Debian

> *Like one of our members, Matt Zimmerman, wrote earlier today:*
>
> *pool/main/o/openssh/openssh_3.4p1.orig.tar.gz*
> *has md5sum 459c1d0262e939d6432f193c7a4ba8a8*
> *this refers to Debian GNU/Linux 3.0 (woody)*
>
> *dists/potato/updates/main/source/openssh_3.4p1.orig.tar.gz*
> *has md5sum 459c1d0262e939d6432f193c7a4ba8a8*
> *this refers to Debian GNU/Linux 2.2 (potato)*
>
> *security.debian.org/pool/updates/main/o/openssh/openssh_3.4p1.orig.tar.gz*
> *has md5sum 459c1d0262e939d6432f193c7a4ba8a8*
> *this refers to our security updates*
>
> *all of which match the FreeBSD one, not the trojaned version.*
> *They also match this signature:*
>
> *ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-3.4p1.tar.gz.sig*
>
> *from this key:*
>
> *pub 1024D/86FF9C48 2001-02-26 Damien Miller (Personal Key) <djm@mindrot.org>*
> *Key fingerprint =3D 3981 992A 1523 ABA0 79DB FC66 CE8E CB03 86FF 9C48*
> *sub 2048g/AA2B1C41 2001-02-26*

NetBSD

> *Both the OpenSSH in the base NetBSD system, and the OpenSSH distribution files available from ftp.netbsd.org have never been compromised with this trojan code.*
>
> *NetBSD mirror sites retrieve their copy from ftp.netbsd.org, and so they would also be unaffected.*
>
> *NetBSD pkgsrc compares downloaded distribution files against a known-good SHA1 hash to prevent the use of trojaned distribution files.*

Nortel Networks

> *Nortel Networks products and solutions are not affected by the vulnerability identified in CERT Advisory CA-2002-24.*

IBM Corporation

> *IBM's AIX operating system does not ship with OpenSSH; however, OpenSSH is available for installation on AIX via the Linux Affinity Toolkit. The packages currently available on the website do not contain the trojan code. We have verified that our OpenSSH packages were generated from clean source packages from the OpenSSH organization.*

MandrakeSoft

> *MandrakeSoft has verified that the openssh-3.4p1 sources used to build it's latest updates (ref. MDKSA-2002:040-1) do not contain this trojan.*

Feedback can be directed to the author: Chad Dougherty.

Revision History

```
August 1, 2002: Initial release
August 1, 2002: Added IBM vendor statement
August 2, 2002: Added Debian, NetBSD, and Nortel vendor statements
```