

SSH exploit

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-12/0189.html>

From: Paul J. Richardson (paul.j.richardson_at_earthlink.net)

Date: 12/22/03

Date: Mon, 22 Dec 2003 02:11:49 GMT

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

Hash: SHA1

Hi,

My professor (NCSU) wants me to hack his honeynet box (it's on the internet, but I can't give anyone the IP), but I'm somewhat new to Linux, and barely read uncompiled script. My only hope (if even relevant?), is I know a bit about TCP/IP and crypto. He flat told me SSH was my best hope of getting in.

A peripheral issue is that (except for one tool at packetstormsecurity.nl), I can't find the tools/scripts described at places such as http://www.totse.com/en/hack/hack_attack/162684.html

thanks much,
Paul

Here's what a Nessus scan shows:

You are running a version of OpenSSH which is older than 3.7.1

Versions older than 3.7.1 are vulnerable to a flaw in the buffer management

functions which might allow an attacker to execute arbitrary commands on this

host.

An exploit for this issue is rumored to exist.

Note that several distribution patched this hole without changing

comp.security.ssh: SSH exploit

the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :

```
rpm -q openssh-server
```

Returns :

```
openssh-server-3.1p1-13 (RedHat 7.x)
```

```
openssh-server-3.4p1-7 (RedHat 8.0)
```

```
openssh-server-3.5p1-11 (RedHat 9)
```

Solution : Upgrade to OpenSSH 3.7.1

See also :

<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2>

<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2>

Risk factor : High

CVE : CAN-2003-0693, CAN-2003-0695

BID : 8628

You are running a version of OpenSSH older than OpenSSH 3.2.1

A buffer overflow exists in the daemon if AFS is enabled on

your system, or if the options KerberosTgtPassing or

AFSTokenPassing are enabled. Even in this scenario, the

vulnerability may be avoided by enabling UsePrivilegeSeparation.

Versions prior to 2.9.9 are vulnerable to a remote root

exploit. Versions prior to 3.2.1 are vulnerable to a local

root exploit.

Solution :

SSH exploit

Upgrade to the latest version of OpenSSH

Risk factor : High

CVE : CVE-2002-0575, CAN-2002-0575

BID : 4560

You are running a version of OpenSSH which is older than 3.1.

Versions prior than 3.1 are vulnerable to an off by one error that allows local users to gain root access, and it may be possible for remote users to similarly compromise the daemon for remote access.

In addition, a vulnerable SSH client may be compromised by connecting to a malicious SSH daemon that exploits this vulnerability in the client code, thus compromising the client system.

Solution : Upgrade to OpenSSH 3.1 or apply the patch for prior versions. (See: <http://www.openssh.org>)

Risk factor : High

CVE : CVE-2002-0083

BID : 4241

You are running a version of OpenSSH which is older than 3.0.1.

Versions older than 3.0.1 are vulnerable to a flaw in which an attacker may authenticate, provided that Kerberos V support has been enabled (which is not the case by default).

It is also vulnerable as an excessive memory clearing bug,

believed to be unexploitable.

*** You may ignore this warning if this host is not using

*** Kerberos V

Solution : Upgrade to OpenSSH 3.0.1

Risk factor : Low (if you are not using Kerberos) or High (if kerberos is enabled)

CVE : CVE-2002-0083

BID : 3560, 4560, 4241

You are running a version of OpenSSH which is older than 3.4

There is a flaw in this version that can be exploited remotely to give an attacker a shell on this host.

Note that several distribution patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :

```
rpm -q openssh-server
```

Returns :

```
openssh-server-3.1p1-6
```

Solution : Upgrade to OpenSSH 3.4 or contact your vendor for a patch

Risk factor : High

CVE : CVE-2002-0639, CVE-2002-0640, CAN-2002-0639, CAN-2002-0640

BID : 5093

comp.security.ssh: SSH exploit

You are running a version of OpenSSH which is older than 3.0.2.

Versions prior than 3.0.2 are vulnerable to an environment

variables export that can allow a local user to execute

command with root privileges.

This problem affect only versions prior than 3.0.2, and when

the UseLogin feature is enabled (usually disabled by default)

Solution : Upgrade to OpenSSH 3.0.2 or apply the patch for prior

versions. (Available at: <ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH>)

Risk factor : High (If UseLogin is enabled, and locally)

CVE : CVE-2001-0872

BID : 3614

You are running a version of SSH which is

older than version 1.2.32,

or a version of OpenSSH which is older than

2.3.0.

This version is vulnerable to a flaw which allows

an attacker to gain a root shell on this host.

Solution :

Upgrade to version 1.2.32 of SSH which solves this problem,

or to version 2.3.0 of OpenSSH

More information:

http://www.core-sdi.com/advisories/ssh1_deattack.htm

Risk factor : High

CVE : CVE-2001-0144

BID : 2347

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

Version: PGP 8.0.3

iQA/AwUBP+ZS2ivoGtpSILwREQJIOACgrizRM2XhNGz3aO9sm1yGuQfbWhUAn0Fy

UTNKCgyIZalVZuWJAeY8s9Z3

=QtOB

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