[prev in list] [next in list] [prev in thread] [next in thread]

List: openbsd-security-announce
Subject: Announce: OpenSSH 6.6 released
From: Damien Miller <djm () mindrot ! org>
Date: 2014-03-15 21:41:41
Message-ID: alpine.BSO.2.11.1403160840320.21113 () natsu ! mindrot ! org
[Download RAW message or body]

OpenSSH 6.6 has just been released. It will be available from the mirrors listed at http://www.openssh.com/ shortly.

OpenSSH is a 100% complete SSH protocol version 1.3, 1.5 and 2.0 implementation and includes sftp client and server support.

Once again, we would like to thank the OpenSSH community for their continued support of the project, especially those who contributed code or patches, reported bugs, tested snapshots or donated to the project. More information on donations may be found at: http://www.openssh.com/donations.html

Changes since OpenSSH 6.6
=========================

This is primarily a bugfix release.

Security:

* sshd(8): when using environment passing with a sshd_config(5) AcceptEnv pattern with a wildcard. OpenSSH prior to 6.6 could be tricked into accepting any enviornment variable that contains the characters before the wildcard character.

New / changed features:

* ssh(1), sshd(8): this release removes the J-PAKE authentication code. This code was experimental, never enabled and had been unmaintained for some time.

* ssh(1): when processing Match blocks, skip 'exec' clauses other clauses predicates failed to match.

* ssh(1): if hostname canonicalisation is enabled and results in the destination hostname being changed, then re-parse ssh_config(5) files using the new destination hostname. This gives 'Host' and 'Match' directives that use the expanded hostname a chance to be applied.

Bugfixes:

* ssh(1): avoid spurious "getsockname failed: Bad file descriptor" in ssh -W. bz#2200, debian#738692

* sshd(8): allow the shutdown(2) syscall in seccomp-bpf and systrace sandbox modes, as it is reachable if the connection is terminated during the pre-auth phase.

```
  * ssh(1), sshd(8): fix unsigned overflow that in SSH protocol 1 bignum
    parsing. Minimum key length checks render this bug unexploitable to
    compromise SSH 1 sessions.

  * sshd_config(5): clarify behaviour of a keyword that appears in
    multiple matching Match blocks. bz#2184

  * ssh(1): avoid unnecessary hostname lookups when canonicalisation is
    disabled. bz#2205

  * sshd(8): avoid sandbox violation crashes in GSSAPI code by caching
    the supported list of GSSAPI mechanism OIDs before entering the
    sandbox. bz#2107

  * ssh(1): fix possible crashes in SOCKS4 parsing caused by assumption
    that the SOCKS username is nul-terminated.

  * ssh(1): fix regression for UsePrivilegedPort=yes when BindAddress is
    not specified.

  * ssh(1), sshd(8): fix memory leak in ECDSA signature verification.

  * ssh(1): fix matching of 'Host' directives in ssh_config(5) files
    to be case-insensitive again (regression in 6.5).

Portable OpenSSH:

  * sshd(8): don't fatal if the FreeBSD Capsicum is offered by the
    system headers and libc but is not supported by the kernel.
  * Fix build using the HP-UX compiler.

Checksums:
==========

  - SHA1 (openssh-6.6.tar.gz) = bf932d798324ff2502409d3714d0ad8d65c7e1e7
  - SHA256 (openssh-6.6.tar.gz) = jaSJE5aiQRm+91dV6EvVGr/ozo33tbxyjjFSiu+Cy80=

  - SHA1 (openssh-6.6p1.tar.gz) = b850fd1af704942d9b3c2eff7ef6b3a59b6a6b6e
  - SHA256 (openssh-6.6p1.tar.gz) = SMHwZktFNIdQOABMxPNVW4MpwqgcHfSNtcUXgA3iA7s=

Please note that the PGP key used to sign releases was recently rotated.
The new key has been signed by the old key to provide continuity. It is
available from the mirror sites as RELEASE_KEY.asc.

Reporting Bugs:
===============

- Please read http://www.openssh.com/report.html
  Security bugs should be reported directly to openssh@openssh.com

OpenSSH is brought to you by Markus Friedl, Niels Provos, Theo de Raadt,
Kevin Steves, Damien Miller, Darren Tucker, Jason McIntyre, Tim Rice and
Ben Lindstrom.
```

[prev in list] [next in list] [prev in thread] [next in thread]