dropbear / CHANGES

mkj 2025.88 changelog ✓ 8872416 · yesterday

1966 lines (1275…

Code Blame Raw

```
2025.88 - 7 May 2025

- Security: Don't allow dbclient hostname arguments to be interpreted
  by the shell.

  dbclient hostname arguments with a comma (for multihop) would be
  passed to the shell which could result in running arbitrary shell
  commands locally. That could be a security issue in situations
  where dbclient is passed untrusted hostname arguments.

  Now the multihop command is executed directly, no shell is involved.
  Thanks to Marcin Nowak for the report, tracked as CVE-2025-47203

- Fix compatibility for htole64 and htole32, regression in 2025.87
  Patch from Peter Fichtner to work with old GCC versions, and
  patch from Matt Robinson to check different header files.

- Fix building on older compilers or libc that don't support
  static_assert(). Regression in 2025.87

- Support ~R in the client to force a key re-exchange.

- Improve strict KEX handling. Dropbear previously would allow other
  packets at the end of key exchange prior to receiving the remote
  peer's NEWKEYS message, which should be forbidden by strict KEX.
  Reported by Fabian Bäumer.

2025.87 - 5 March 2025

Note >> for compatibility/configuration changes

- >> Disable SHA-1 algorithms by default. SHA-1 has known weakness and
  most implementations support alternatives

- Add post-quantum key exchange. These avoid the possibility of current
  stored traffic being decrypted using a possible future quantum
```

```
  computer.

  sntrup761 added by Matt Johnston, using sntrup761 implementation from
  Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange and
  Christine van Vredendaal, with integration work from OpenSSH.

  ML-KEM added by Loganaden Velvindron, Jaykishan Mutkawoa, Kavish Nadan,
  using libcrux, also based on OpenSSH work.

  These do increase code size, at least sntrup761 is recommended,
  see default_options.h

- >> Decompression is disabled on the server, compression
  is still supported.
  This avoids attack surface for zlib and saves runtime memory.

- Add -D server flag to specify authorized_keys directory, from Darren Tucker.

- Include remote host in "Login attempt with wrong user" message for fail2ban,
  patch from MichaIng.

- Workaround writing hostkeys on FUSE filesystem that don't
  support hardlinks, reported by elijahr.

- Fix truncated error messages such as host key mismatch.

- >> Preference aes256 ahead of aes128 for the client. chacha20-poly1305
  is still first preference.

- Fix ubsan failure in curve25519 code, reported by Steven Bytnar.
  Has no effect on execution.

2024.86 - 22 October 2024

- Fix failure on concurrent channel open/close.
  This was a regression in 2022.82, reported by rsflo in Github #321.
    failed assertion in common-channel.c:705: !channel->sent_close

- Print remote host after "Login attempt for nonexistent user" log entry to
  assist fail2ban. Fix from MichaIng, the format changed in 2020.79

- Dropbear now exits with exit status 0 on SIGINT/SIGTERM. This is a more
  graceful behaviour for "systemctl stop dropbear".
  Reported by Ninad Palsule

- New IDENT_VERSION_PART config allows customising some of the SSH version
  string. From Marius Dinu

- Fix building SK_KEYS with just one of ECDSA or ED25519
  From Marius Dinu

- Fix dbclient "-m help" and "-c help" without a hostname.
  Patch from Darren Tucker
```

```
- Remove fprintf/gettimeofday from sigchld handler when running with
  verbose trace enabled.

- Improved configure help output, from Mikel Olasagasti Uranga

- Compile fix for GNU Hurd, from Guilhem Moulin

- Support running test_aslr without venv, from Guilhem Moulin

- Compilation fixes for older compilers, and better build tests

- Update some test infrastructure versions of python packages,
  github actions, and github runner OSes

2024.85 - 25 April 2024

  This release fixes build regressions in 2024.84

- Fix build failure when SHA1 is disabled, thanks to Peter Krefting

- Fix build failure when DROPBEAR_CLI_PUBKEY_AUTH disabled, thanks to
  Sergey Ponomarev

- Update debian/ directory with changed paths

2024.84 - 4 April 2024

Features and Changes:
  Note >> for compatibility/configuration changes

- >> Only use /etc/shadow when a user has :x: as the crypt in /etc/passwd.
  This is the documented behaviour of passwd(5) so should be consistent with
  other programs. Thanks to Paulo Cabral for the report.
  Note that any users without x as the crypt will not be able
  to log in with /etc/shadow, in cases were the existing configuration
  differs.

- Support -o StrictHostKeyChecking, patch from Sergey Ponomarev

- Support -o BatchMode, from Sergey Ponomarev and Hans Harder

- Support various other -o options compatible with OpenSSH, from
  Sergey Ponomarev. Includes -o PasswordAuthentication
```

```
1893      (noticed by Davyd Madeley <davyd at zdlcomputing.com>)
1894    - Added initial tcp forwarding code, only -L (local) at this stage
1895    - Improved "make install" with DESTDIR and changing ownership seperately,
1896      don't check for setpgrp on Linux for crosscompiling.
1897      (from Erik Andersen <andersen at codepoet.org>)
1898    - More commenting, fix minor compile warnings, make return values more
1899      consistent etc
1900    - Various signedness fixes
1901    - Can listen on multiple ports
1902    - added option to disable openpty with configure script,
1903      (from K.-P. Kirchdörfer <kapeka at epost.de>)
1904    - Various cleanups to bignum code
1905      (thanks to Tom St Denis <tomstdenis at iahu.ca>)
1906    - Fix compile error when disabling RSA
1907      (from Marc Kleine-Budde <kleine-budde at gmx.de>)
1908    - Other cleanups, splitting large functions for packet and kex handling etc
1909
1910    0.33 - Sun June 22 2003 22:24:12 +0800
1911
1912    - Fixed some invalid assertions in the channel code, fixing the server dying
1913      when forwarding X11 connections.
1914    - Add dropbearconvert to convert to/from OpenSSH host keys and Dropbear keys
1915    - RSA keys now keep p and q parameters for compatibility -- old Dropbear keys
1916      still work, but can't be converted to OpenSSH etc.
1917    - Debian packaging directory added, thanks to
1918      Grahame (grahame at angrygoats.net)
1919    - 'install' target added to the makefile
1920    - general tidying, improve consistency of functions etc
1921    - If RSA or DSS hostkeys don't exist, that algorithm won't be used.
1922    - Improved RSA and DSS key generation, more efficient and fixed some minor bugs
1923      (thanks to Tom St Denis for the advice)
1924    - Merged new versions of LibTomCrypt (0.86) and LibTomMath (0.21)
1925
1926    0.32 - Sat May 24 2003 12:44:11 +0800
1927
1928    - Don't compile unused code from libtomcrypt (test vectors etc)
1929    - Updated to libtommath 0.17 and libtomcrypt 0.83. New libtommath results
1930      in smaller binary size, due to not linking unrequired code
1931    - X11 forwarding added
1932    - Agent forwarding added (for OpenSSH.com ssh client/agent)
1933    - Fix incorrect buffer freeing when banners are used
1934    - Hostname resolution works
1935    - Various minor bugfixes/code size improvements etc
1936
1937    0.31 - Fri May 9 2003 17:57:16 +0800
```

```
    - Improved syslog messages - IP logging etc
    - Strip control characters from log messages (specified username currently)
    - Login recording (utmp/wtmp) support, so last/w/who work - taken from OpenSSH
    - Shell is started as a proper login shell, so /etc/profile etc is sourced
    - Ptys work on Solaris (2.8 x86 tested) now
    - Fixed bug in specifying the rsa hostkey
    - Fixed bug in compression code, could trigger if compression resulted in
      larger output than input (uncommon but possible).

    0.30 - Thu Apr 17 2003 18:46:15 +0800

    - SECURITY: buffer.c had bad checking for buffer increment length - fixed
    - channel code now closes properly on EOF - scp processes don't hang around
    - syslog support added - improved auth/login/failure messages
    - general code tidying, made return codes more consistent
    - Makefile fixed for dependencies and makes libtomcrypt as well
    - Implemented sending SSH_MSG_UNIMPLEMENTED :)

    0.29 - Wed Apr 9 2003

    - Fixed a stupid bug in 0.28 release, 'newstr = strdup(oldstr)',
      not 'newstr=oldstr'

    0.28 - Sun Apr 6 2003

    - Initial public release

    Development was started in October 2002
```