

---

Subject: SSH package is upgraded to libssh2 v1.9.0  
Posted by [Oblivion](#) on Tue, 17 Nov 2020 15:34:43 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Hi,

libssh2, the SSH2 engine of SSH package is upgraded to v1.9  
Package is tested with GCC/CLANG/MSVC19, Linux and Windows 7/10.

- o adds ECDSA keys and host key support when using OpenSSL
- o adds ED25519 key and host key support when using OpenSSL 1.1.1
- o adds OpenSSH style key file reading
- o adds AES CTR mode support when using WinCNG
- o adds PEM passphrase protected file support for Libgcrypt and WinCNG
- o adds SHA256 hostkey fingerprint
- o adds libssh2\_agent\_get\_identity\_path() and libssh2\_agent\_set\_identity\_path()
- o adds explicit zeroing of sensitive data in memory
- o adds additional bounds checks to network buffer reads
- o adds the ability to use the server default permissions when creating sftp directories
- o adds support for building with OpenSSL no engine flag
- o adds support for building with LibreSSL
- o increased sftp packet size to 256k
- o fixed oversized packet handling in sftp
- o fixed building with OpenSSL 1.1
- o fixed a possible crash if sftp stat gets an unexpected response
- o fixed incorrect parsing of the KEX preference string value
- o fixed conditional RSA and AES-CTR support
- o fixed a small memory leak during the key exchange process
- o fixed a possible memory leak of the ssh banner string
- o fixed various small memory leaks in the backends
- o fixed possible out of bounds read when parsing public keys from the server
- o fixed possible out of bounds read when parsing invalid PEM files
- o no longer null terminates the scp remote exec command
- o now handle errors when diffie hellman key pair generation fails

Notes:

- Since I don't have a Mac, I couldn't test it on MacOS. Any feedback on that front will be appreciated.

- MSVC19 warns about implicit ssize\_t/size\_t -> int cast. In our specific case, this is harmless. Still I might suppress or try to fix these warnings before the official U++ 2021.1 release.

Best regards,  
Oblivion

