# OpenSSH 6.9 Portable released

Contributed by Michael Felt

-

OpenSSH 6.9 has been released. This release is primarily a bugfix release. The bigger news is about the plans for release 7.0 expected in Late July (2015).
- Note - also available as "LibreSSH" - OpenSSH linked against LibreSSL rather than OpenSSL.

From the release notes:
The 7.0 release of OpenSSH, due for release in late July, will deprecate several features, some of which may affect compatibility or existing configurations.

The intended changes are as follows:

- The default for the sshd_config(5) PermitRootLogin option will change from "yes" to "no".

- Support for the legacy version 1.x of the SSH protocol will be disabled at compile time by default.

- Support for the 1024-bit diffie-hellman-group1-sha1 key exchange will be run-time disabled by default.

- Support for ssh-dss, ssh-dss-cert-* host and user keys will be run-time disabled by default.

- Support for the legacy v00 cert format will be removed

- Several ciphers will be disabled by default: blowfish-cbc, cast128-cbc, all arcfour variants and the rijndael-cbc aliases for AES

- Refusing all RSA keys smaller than 1024 bits (the current minimum is 768 bits)

This list reflects our current intentions, but please check the final release notes for OpenSSH 7.0 when it is released.