OpenSSH release Notes (since 6.0)

Contributed by Michael Felt

A lot has changed since OpenSSH-6.0 was released. Why worry about OpenSSH-6.0? Because that is the basis for the core functions and options provided by the current AIX openssh.base. As I understand the IBM packaging - the current, better would be to say latest - is based on OpenSSH-6.0. OpenSSH-7.1 and OpenSSH-7.5 and these include patches to 'repair' CVE issues.These can be downloaded via: AIX Web Download Pack Programs

FYI: The current OpenSSH release is OpenSSH-7.6.I have this packaged and available for download from http://www.aixtools.net/index.php/openssh

OpenSSH is released in two versions: regular (for OpenBSD) and "portable" (for the rest of us). The portable release is recognized by adding p1 (sometimes p2) after the release name, e.g., OpenSSH-6.0p1 or OpenSSH-7.6p1.

The table shows name, release date and a "few word summary". The release name links to the release document.

RELEASE NOTES	RELEASED	SUMMARY
release-6.0	21-Apr-2012	bugfix
release-6.1	28-Aug-2012	bugfix
release-6.2	21-Mar-2013	new features bugfix
release-6.2p2	15-May-2013	bugfix

release-6.3
13-Sep-2013
bugfix

new features

release-6.4
07-Nov-2013
security

release-6.5
30-Jan-2014
new features

bugfix

release-6.6
15-Mar-2014
bugfix

security

release-6.7
06-Oct-2014
compatibility:

modify default ciphers and MACs

new features

bugfix

release-6.8
17-Mar-2015
MAJOR RELEASE

new features

bugfixes

compatibility:

UseDNS=no

release-6.9
30-Jun-2015
bugfix

new features

release-7.0
11-Aug-2015

FOCUS:

deprecate weak, legacy and/or unsafe cryptography

support for SSHv1 disabled

support for DSA (ssh-dss) disabled

compatibility:

PermitRootLogin: new options, new default

bugfix

release-7.1
21-Aug-2015
bugfix

release-7.1p2
14-Jan-2016
security

release-7.2
28-Feb-2016
bugfix

features

security

release-7.2p2
10-Mar-2016
security

release-7.3
01-Aug-2016
bugfix

security

features

release-7.4
19-Dec-2016
compatibility:

SSHv1 support removed

remove 3des-cbc from client proposal

bugfix

features

release-7.5
20-Mar-2017
compatibility:

no (build) support for prior to OpenSSL 1.0.2

bugfix

new features

release-7.6
04-Oct-2017

compatibility:

Potentially-incompatible changes

no support for old ciphers and RSA keys <1024 bits

bugfix

new features