SSH-01-Fix-Verification

The following lines enumerate the fix-verification work for SSH-01 by Cure53.

SSH-01-003 Client: Missing *NULL* check leads to crash in erroneous state *(Low)*

- *ssh_packet_get_current_crypto* explicitly initializes the *crypto* before returning
- The switch/case makes sure that *out_cipher* and *in_cipher* are set whatever direction is used
- **VERIFIED FIXED**

SSH-01-004 SCP: Unsanitized location leads to command execution (***Critical***)

- Functionality is extended to include a method called *ssh_quote_file_name* that implements different states to know when quoting is necessary
- Initialization routines make sure that *ssh_quote_file_name* is called early on the scp-location
- Additional test cases to torture *ssh_quote_file_name* are implemented. Covers edgecase, small and large buffers. Looks sane.
- This is also disclosed as CVE-2019-14889.
- **VERIFIED FIXED**

SSH-01-006 General: Various unchecked *Null-derefs* cause DOS *(Low)*

- They actually went through each of the semmle findings and included a == *NULL* bailout for each case
- **VERIFIED FIXED**

SSH-01-007 PKI Gcrypt: Potential UAF/double free with RSA pubkeys *(Medium)*

- Instead of calling *ssh_string_free* the *SSH_STRING_FREE* macro is used
- This is actually quite elegant because the macro expansion makes sure the elements are correctly set to NULL this way, instead of losing the pointer when calling *ssh_string_free* originally.
- **VERIFIED FIXED**

SSH-01-010 SSH: Deprecated hash function in fingerprinting *(Low)*

- Insecure hashes are still kept for backwards compatibility, understandable

- Instead the user is warned to move to a better fingerprint hash they offer
- Still, having backwards compatibility does not help in going forward and improving the basis. This is somewhat of an ethics question though i suppose
- **PARTIALLY VERIFIED**

SSH-01-011 SSH: Lack of point validation on *X25519* and *Ed25519* (*Medium*)

- *"Note that we consider SSH-001-011 as invalid, at least for curve25519 used for the KEX! Feel free to join the discussion in https://bugs.libssh.org/T185"*
- **NOT VERIFIED**

SSH-01-013 Conf-Parsing: Recursive wildcards in hostnames lead to DOS (*Low*)

- The patch implements a recursion limit with *MAX_MATCH_RECURSION* set to 32 to make sure that *match_pattern* won't smash the stack
- Looks fine
- **VERIFIED FIXED**

SSH-01-014 Conf-Parsing: Integer underflow leads to OOB array access (*Low*)

- Empty lines are correctly ignored
- This should take care of the oob issue
- **VERIFIED FIXED**

SSH-01-002 Kex: Differently bound macros used to iterate same array (*Info*)

- Functionality is now consistent in using *SSH_KEX_METHODS*
- **VERIFIED FIXED**

SSH-01-005 Code-Quality: Integer sign confusion during assignments (*Low*)

- This is a huge patch, where it looks like they went through each of the semmle outputs and made sure to keep types consistent. There are quite a lot of changes and i am not able to verify them all to 100% but it looks correctly done
  - Ints were mostly changed to size_t
  - Return values that previously were negative were patched to return 0 on failure
  - For some reason they switched native types to sys/types in some occasions in the code but not in all. This is not problematic though, but rather inconsistent.
  - They also enabled *Wsign-compare* in gcc to get ahead of further mistakes during compile time
- **VERIFIED FIXED**

SSH-01-008 SCP: Protocol Injection via unescaped File Names (*Low*)

- The patch does not really implement vis encoding but rather just escapes newlines in path/file names
- This appears to work fine though and should take care of the issue.

- **VERIFIED FIXED**

SSH-01-001 State Machine: Initial machine states should be set explicitly *(Info)*

- This makes sure that the states are explicitly initialized during *ssh_new*
- Channel and opts.flags are explicitly set as well
- **VERIFIED FIXED**

SSH-01-009 SSH: *RFC4255* not Implemented *(Info)*

- Well this just goes the easy route of updating the list of RFCs that are not implemented.
- Fine with us
- **VERIFIED FIXED**

SSH-01-012 PKI: Information leak via uninitialized stack buffer *(Low)*

- Buffers are now correctly set to NULL and {0}
- **VERIFIED FIXED**