zlib SOS Fund Audit Fix Log

Identified Issues

Finding 1: Incompatible declarations for external linkage function deflate (Medium)

Fix: https://github.com/madler/zlib/commit/3fb251b363866417122fe54a158a1ac5a7837101

VERIFIED

Finding 2: Accessing a buffer of char via a pointer to unsigned int (Low)

Mark Adler (zlib): [This] will remain as is. Yes, speed matters a great deal. The comment in the report: "In the longer term, platform specific micro-optimizations should be deprecated. These optimizations may no longer be necessary: modern compilers are much better at optimizing and vectorizing code than they used to be." does not apply. This is not a micro-optimization, and unless the compiler has the intelligence and creativity of a good mathematician well-versed in discrete mathematics, can detect the application of Galois Fields in the code, know somehow to postulate a theorem for an equivalent calculation over GF(2) that will, in the end, improve the speed, prove that theorem, and then generate on its own the additional tables to apply that theorem, then no, there is no way that a compiler is coming up with that one.

UNRESOLVED: *This issue remains under discussion to determine whether there is a way which removes the mismatched pointer without affecting performance.*

Finding 3: Out-of-bounds pointer arithmetic in inftrees.c (Low)

Fix: https://github.com/madler/zlib/commit/6a043145ca6e9c55184013841a67b2fef87e44c0
https://github.com/madler/zlib/commit/9aaec95e82117c1cb0f9624264c3618fc380cecb

VERIFIED

Finding 4: Undefined left shift of negative number (Low)

Fix: https://github.com/madler/zlib/commit/e54e1299404101a5a9d0cf5e45512b543967f958
(This was already fixed on the development branch before being discovered.)

VERIFIED

Finding 5: Big-endian out-of-bounds pointer (Low)

Fix: https://github.com/madler/zlib/commit/d1d577490c15a0c6862473d7576352a9f18ef811

VERIFIED