dovecot SOS Fund Audit Fix Log

Identified Vulnerabilities

DOV-01-001 Format String Protection can be bypassed (Low)

Timo Sirainen (dovecot): We've fixed the detection of %n when various modifiers are used: https://github.com/dovecot/core/commit/4baf980b75800ad3595c39dc3b8d913f2686affd

VERIFIED

Timo Sirainen (dovecot): Additionally, we've added a whitelist of allowed format characters, just to be sure that if a future libc version adds new unknown modifiers they won't be allowed to bypass the %n check: https://github.com/dovecot/core/commit/ebe00087d3c7f9706d4acb9017eaad912404516c

VERIFIED

DOV-01-002 Default Makefile fails to add Hardening Flags (Low)

Timo Sirainen (dovecot): The hardening flags were added to the git master tree (= upcoming v2.3) already in April: https://github.com/dovecot/core/commit/14a7cd46677cc0052319f2cd84a7b720efa60499 although the logic in it was somewhat wrong and was fixed by https://github.com/dovecot/core/commit/fdf3e1e28e824a562b895c8c6b5d77d70146d357

VERIFIED

Timo Sirainen (dovecot): We haven't yet backported these to v2.2 code tree, but that could be a possibility.

Mike Wege (Cure53): *I don't deem it necessary to backport the flags, considering the required testing.*

DOV-01-003 Memorypool Allocator fails to check for Integer Overflows (Low)

Timo Sirainen (dovecot): We attempted to find optimized malloc-overflow checks in existing software but couldn't really find anything. So we implemented our own MALLOC_ADD() and MALLOC_MULTIPLY() macros that panic if an integer overflow occurs: https://github.com/dovecot/core/commit/b716136fc47efd434d60be5db262b4013e375fa9 - these could possibly be further optimized, but it probably doesn't make a big difference. I think most of the if-checks are already optimized away on 64bit systems because two 32bit integer multiplications can't overflow 64bit size_t. We'd be interested to hear any further recommendations.

VERIFIED

Timo Sirainen (dovecot): Based on the MALLOC_MULTIPLY() the [ipt]_new() macros will check for overflows: https://github.com/dovecot/core/commit/7e90e9424489b06ebe17a019f56eb3624ca091b2 - Here as long as the count parameter is 32bit or smaller, the overflow-check gets optimized away on 64bit systems.

VERIFIED

Timo Sirainen (dovecot): We changed hopefully all of the memory size allocations to use MALLOC_*() macros: https://github.com/dovecot/core/commit/e7d0bea63a08b08c47c4b5c187d2cb7127859657 (As noted in the first commit's comments, MALLOC_ADD(n, 1) isn't used because it would always wrap to 0, and *_malloc(0) will already panic. The +1 is also very commonly used.)

VERIFIED

Timo Sirainen (dovecot): Additionally, we noticed that a lot of strlen() calls were stored into "unsigned int" rather than size_t. Although it's pretty unlikely that there exists >4GB strings, it could be a possible attack vector. We've fixed most of these: https://github.com/dovecot/core/commit/2ac5f36aa7c2e7a07ba8815d43a6d7483f62e74c

VERIFIED

Timo Sirainen (dovecot): It likely doesn't fix everything though. Clang's -Wshorten-64-to-32 parameter appears to be a good way to find all of these automatically. We're planning on further patches to fix those warnings as well.

Mike Wege (Cure53): *I commend you for your proactive approach, we didn't even check those warnings.*