Knot DNS SOS Fund Audit Fix Log

Identified Vulnerabilities

A: Non-Cryptographic Hash Used for DNS cookies (Low)

Fixed in https://gitlab.labs.nic.cz/knot/knot-dns/commit/79618ab3de0f9c6f
Will be released in Knot DNS 2.7.0

VERIFIED

Jack Lloyd (Least Authority): *Now SipHash is used.*

B: Timing Channel in DNS Cookie Comparisons (Low)

Fixed in https://gitlab.labs.nic.cz/knot/knot-dns/commit/8666568a408dd696
Released in Knot DNS 2.6.2

VERIFIED

Jack Lloyd (Least Authority): *Now constant time memcmp is used.*

C: Weak RSA keys allowed (Medium)

Fixed in https://gitlab.labs.nic.cz/knot/knot-dns/commit/d0f52e7c40169ef4
Will be released in Knot DNS 2.7.0

VERIFIED

Jack Lloyd (Least Authority): *Now at least 1024-bit RSA is required.*

D: Insufficient Build Hardening (Low)

Daniel Salzman (Knot DNS): Most of the supported systems have specific settings and support of build hardening. Not yet decided which hardening would be universally accepted. We are happy for the audit to be published without further work on this item.

NOT VERIFIED

E: Hash Function Collisions (Medium)

Fixed in https://gitlab.labs.nic.cz/knot/knot-dns/commit/2bae46b8c4df21be
Will be released in Knot DNS 2.7.0

VERIFIED

Jack Lloyd (Least Authority): *Murmur hash replaced by SipHash with random key.*

F: Missing Error Check Causing Crash (Low)

Fixed in https://gitlab.labs.nic.cz/knot/knot-dns/commit/ba084da5bba3bfb3
Released in Knot DNS 2.6.2

VERIFIED

Jack Lloyd (Least Authority): *Value that would cause overflow now checked.*

G: Use of assert macro for error checking (Medium)

Daniel Salzman (Knot DNS): The code is continuously reviewed and refactored to eliminate wrong asserts. Knot DNS 2.7.0 will include improved libknot interface, e.g. knot_dname_size returns unsigned integer. This work is not yet completed, but we are happy for the audit to be published without further work on this item.

NOT VERIFIED

H: Not Checking Return Value For Error (Low)

Removed in https://gitlab.labs.nic.cz/knot/knot-resolver/commit/0c3f6a269e8a4817
Relates to https://gitlab.labs.nic.cz/knot/knot-resolver/issues/108
Released in Knot Resolver 2.0.0

VERIFIED

Jack Lloyd (Least Authority): *Both calls to malloc were removed in the referenced commit (rewite of cache layer).*

I: Weak PRNG (Low)

Relates to https://gitlab.labs.nic.cz/knot/knot-resolver/issues/233

Daniel Salzman (Knot DNS): Not yet fixed. We are happy for the audit to be published without further work on this item.

NOT VERIFIED

J: Integer Overflow (Low)

Fixed in https://gitlab.labs.nic.cz/knot/knot-resolver/commit/0f2318d9df4ff481
Released in Knot Resolver 2.0.0

VERIFIED

Jack Lloyd (Least Authority): *Now overflow is checked.*

K: Integer Overflow (Low)

Removed in https://gitlab.labs.nic.cz/knot/knot-resolver/commit/0c3f6a269e8a4817
Relates to https://gitlab.labs.nic.cz/knot/knot-resolver/issues/108
Released in Knot Resolver 2.0.0

VERIFIED

Jack Lloyd (Least Authority): *Cache code was rewritten, removing the vulnerable code. The integer overflow in kr_stratdup was fixed in commit 0f2318d9df4ff.*

Miscellaneous Issues

1: Redundant Operation (Info)

Fixed in https://gitlab.labs.nic.cz/knot/knot-dns/commit/b330e1da606a0816
Released in Knot DNS 2.6.2

VERIFIED

2: Google's OSS-Fuzz (Info)

Registered as https://github.com/google/oss-fuzz/tree/master/projects/knot-dns

VERIFIED