Fixes for CVE-2025-59088 and CVE-2025-59089 #68

Merged **jrisc** merged 3 commits into `latchset:main` from `jrisc:cve_2025_59088-89` on Nov 14, 2025

jrisc commented on Nov 12, 2025 — Collaborator

This PR fixes two vulnerabilities:

- CVE-2025-59088: Server-side request forgery (SSRF) via DNS discovery
  - Possible because use of DNS SRV records to discovery KDCs was allowed by default for any requested realm
  - Now restricts DNS discovery of KDCs to realms explicitly declared in the configuration only
  - Adds support for wildcard realm sections (e.g., `[*EXAMPLE.COM]`) to handle realm hierarchies (like AD forests)
  - Previous unsafe behavior can be restored using the `dns_realm_discovery` setting
  - A warning is logged if a resolved SRV record points to a non-standard Kerberos port (can be suppressed using the `silence_port_warn` setting)
- CVE-2025-59089: DoS attack via unbounded TCP buffering
  - Possible because of improper message length checks and redundant buffer exports
  - No longer accept messages longer than maximum Kerberos message length
  - Interrupts receiving when incoming message exceeds expected length
  - Export buffer only once after receiving process completed

Also remove outdated MIT license classifier, enable tests for Python 3.12 and 3.14, add missing test dependencies, and do not re-enable implicitly ignored conflicting Flake8 constraints (line breaks before AND after binary operators).

Given the fact this PR has a significant impact on how the configuration of kdcproxy works, it would probably make sense to make it part of a new release.

jrisc added 3 commits 7 months ago

`Fix DoS vulnerability based on unbounded TCP buffering` ··· `93ba737`

`Use DNS discovery for declared realms only` ··· `0254c16`

`Update setup.py and tox.ini` ··· ✓ `e91bdca`

jrisc changed the title ~~**Fixes CVE-2025-59088 and CVE-2025-59089**~~ **Fixes for CVE-2025-59088 and CVE-2025-59089** on Nov 12, 2025

simo5 approved these changes on Nov 12, 2025

View reviewed changes

simo5 left a comment — Member

LGTM

jrisc merged commit **`840cd83`** into `latchset:main` on Nov 14, 2025

View details

8 checks passed

Reviewers

simo5 ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants