Brace for Upgrades – Plural

Petr Špaček (ISC)
Pieter Lexis (PowerDNS)
Benno Overeinder (NLnet Labs)
Vladimír Čunát (CZ.NIC)
Ondřej Surý (ISC)

2026-05-17

pspacek@isc.org

What's happening

- LLMs can find bugs
  - Subset real
    - Subset exploitable

The Problem – Motivation

- CVE = Curriculum Vitae Enhancer
- KPI = number of CVE# assigned
  - Quantity over quality
    - Throw at the wall and see what sticks
- **Not** helping the open-source

BIND

- 2025
  - 4 security releases
  - 8 CVE
- 2026 up to May 20
  - 3 security releases
  - 11 CVEs
    - 130 external reports triaged, 20 more to go
  - 500 more internal finds to triage

< 10 % valid CVE reports

Unbound

- 2025
  - 3 security releases
  - 3 CVEs
- 2026 up to May 20
  - 11 CVEs
  - 40 more external reports to triage

PowerDNS + dnsdist

- 2025
  - 8 CVEs
- 2026 up to today
  - 5 security releases
  - 30 CVEs
  - hundred to triage

~ 5 % valid CVE reports

Consequences

- DoS on development teams
  - Handful of people!
- Feature development delayed
- Less details
  - Workarounds
  - Versions affected
- Tests available with fix

Upgrade cycle

Every two weeks?!

Optimize deployment processes!

Embargos / early notification

- If LLM found it once …
- Risk of independent re-discovery
  - Embargos not upheld

See also

- https://lwn.net/Articles/1070698/
  - Linux: "**users must upgrade to the latest release**"
- https://lists.thekelleys.org.uk/pipermail/dnsmasq-discuss/2026q2/018471.html
- https://www.microsoft.com/en-us/msrc/blog/2026/05/a-note-on-patch-tuesday

Researchers – help us out!

- **Verify** reports you send in
  - Template
    https://gitlab.isc.org/isc-projects/bind9/-/raw/main/.gitlab/issue_templates/Security_issue.md
- Describe threat model
  - **Verify** it matches DNS
    - Malicious parent zone does not count!
- Write regression test
- Think of resource asymmetry

What next

- Hug your OSS maintainer
  - … or support them with a contract
- Brace for **frequent** upgrades