CVE-2026-28810

Predictable DNS Transaction IDs Enable Cache Poisoning in Built-in Resolver

« Back to all CVEs

See on OSV.dev »

Weakness Type (CWE)

CWE-340 — CWE-340 Generation of Predictable Numbers or Identifiers

CAPEC

CAPEC-142 — CAPEC-142 DNS Cache Poisoning

CVSS 4.0 Score

6.3

MEDIUM

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Vulnerability description

Generation of Predictable Numbers or Identifiers vulnerability in Erlang/OTP kernel (inet_res, inet_db modules) allows DNS Cache Poisoning.
The built-in DNS resolver (`inet_res`) uses a sequential, process-global 16-bit transaction ID for UDP queries and does not implement source port randomization. Response validation relies almost entirely on this ID, making DNS cache poisoning practical for an attacker who can observe one query or predict the next ID. This conflicts with RFC 5452 recommendations for mitigating forged DNS answers.

`inet_res` is intended for use in trusted network environments and with trusted recursive resolvers. Earlier documentation did not clearly state this deployment assumption, which could lead users to deploy the resolver in environments where spoofed DNS responses are possible.

This vulnerability is associated with program files `lib/kernel/src/inet_db.erl` and `lib/kernel/src/inet_res.erl`.

This issue affects OTP from OTP 17.0 until OTP 28.4.2, 27.3.4.10 and 26.2.5.19 corresponding to kernel from 3.0 until 10.6.2, 10.2.7.4 and 9.2.4.11.

Affected

`pkg:otp/kernel`

Module	Source File
inet_res	src/inet_db.erl
inet_db	src/inet_res.erl

Status	Type	Version	Changes / Fixed in
Affected	otp ⓘ	`3.0`	• unaffected at `10.6.2` • unaffected at `10.2.7.4` • unaffected at `9.2.4.11`

pkg:github/erlang/otp

Module	Source File
inet_res	lib/kernel/src/inet_db.erl
inet_db	lib/kernel/src/inet_res.erl

Status	Type	Version	Changes / Fixed in
Affected	otp ⓘ	17.0	• unaffected at 28.4.2 • unaffected at 27.3.4.10 • unaffected at 26.2.5.19
Affected	git ⓘ	07b8f441ca	• unaffected at 36f23c9d2c • unaffected at dd15e8eb03 • unaffected at b057a9d995

Configurations

The application must use `inet_res` for DNS resolution, either by configuring the lookup method to include `dns` in the kernel inet configuration, or by calling `inet_res` functions directly. The default Erlang/OTP configuration uses native OS resolution and is not affected.

Workarounds

Install the Erlang nodes in a trusted network shielded from DNS reply spoofing by firewalls, and configure the `inet_res` resolver to only talk to trusted recursive name servers within that network.

References

- https://github.com/erlang/otp/security/advisories/GHSA-v884-5jg5-whj8 vendor-advisory related
- https://osv.dev/vulnerability/EEF-CVE-2026-28810 related
- https://github.com/erlang/otp/commit/36f23c9d2cc54afe83671dd7343596d7972839a5 patch
- https://github.com/erlang/otp/commit/dd15e8eb03548c5e55e9915f0e91389ec6bad9fd patch
- https://github.com/erlang/otp/commit/b057a9d995017b1be50d6dc02edd52382f3231b8 patch

Credits

- **Reporter**: Luigino Camastra / Aisle Research
- **Remediation developer**: Raimo Niskanen

CVE record as JSON: GET /cves/CVE-2026-28810.json
OSV record as JSON: GET /osv/EEF-CVE-2026-28810.json