



# EEF-CVE- 2026-28810

[See a problem?](#)

Please try reporting it [to the source](#) [↗](#) first.

Source	<a href="https://cna.erlef.org/osv/EEF-CVE-2026-28810.html">https://cna.erlef.org/osv/EEF-CVE-2026-28810.html</a> <a href="#">↗</a>
Import Source	<a href="https://cna.erlef.org/osv/EEF-CVE-2026-28810.json">https://cna.erlef.org/osv/EEF-CVE-2026-28810.json</a> <a href="#">↗</a>
JSON Data	<a href="https://api.osv.dev/v1/vulns/EEF-CVE-2026-28810">https://api.osv.dev/v1/vulns/EEF-CVE-2026-28810</a> <a href="#">↗</a>
Aliases	CVE-2026-28810 GHSA-v884-5jg5-whj8
Published	2026-04-07T07:50:11.072Z
Modified	2026-04-07T08:11:26.608014947Z
Severity	<b>6.3 (Medium)</b> CVSS_V4 - 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 <a href="#">CVSS Calculator</a> <a href="#">↗</a>

## Summary

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

## Details

Generation of Predictable Numbers or Identifiers vulnerability in Erlang/OTP kernel (*inetres*, *inetdb* 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/inetdb.erl* and *lib/kernel/src/inetres.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.

**Database specific** [↗](#)

```
{
  "cpe_ids": [
    "cpe:2.3:a:erlang:erlang\\\/otp:*:*:*:*:*:*:*"
  ],
  "capec_ids": [
    "CAPEC-142"
  ],
  "cwe_ids": [
    "CWE-340"
  ]
}
```

## References

<https://github.com/erlang/otp/security/advisories/GHSA-v884-5jg5-whj8> [↗](#)

<https://cna.erlef.org/cves/CVE-2026-28810.html> [↗](#)

<https://www.erlang.org/doc/system/versions.html#order-of-versions> [↗](#)

<https://github.com/erlang/otp/commit/36f23c9d2cc54afe83671dd7343596d7972839a5> [↗](#)

<https://github.com/erlang/otp/commit/dd15e8eb03548c5e55e9915f0e91389ec6bad9fd> [↗](#)

<https://github.com/erlang/otp/commit/b057a9d995017b1be50d6dc02edd52382f3231b8> [↗](#)

## Credits

Luigino Camastra / Aisle Research - REPORTER

Raimo Niskanen - REMEDIATION\_DEVELOPER

## Affected packages


**Git**  
[github.com/erlang/otp](https://github.com/erlang/otp)

## Affected ranges [↗](#)

Type	GIT
Repo	<a href="https://github.com/erlang/otp">https://github.com/erlang/otp</a>
Events	Introduced <a href="https://github.com/erlang/otp/commit/07b8f441ca711f9812fad9e9115bab3c3aa92f79">07b8f441ca711f9812fad9e9115bab3c3aa92f79</a> <a href="#">↗</a> Fixed

[36f23c9d2cc54afe83671dd7343596d7972839a5](#) 

Fixed

[dd15e8eb03548c5e55e9915f0e91389ec6bad9fd](#) 

Fixed

[b057a9d995017b1be50d6dc02edd52382f3231b8](#) 

---

## Affected versions

- ▶ OTP-17.\*
- ▶ OTP-18.\*
- ▶ OTP-19.\*
- ▶ OTP-20.\*
- ▶ OTP-21.\*
- ▶ OTP-22.\*
- ▶ OTP-23.\*
- ▶ OTP-24.\*
- ▶ OTP-25.\*
- ▶ OTP-26.\*
- ▶ OTP-27.\*
- ▶ OTP-28.\*
- ▶ OTP-29.\*
- ▶ Other

---

## Database specific

▶ source

---