EEF-CVE-2026-28810

See a problem?
Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2026-28810.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-28810.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-28810
Aliases	CVE-2026-28810 GHSA-v884-5jg5-whj8
Published	2026-04-07T07:50:11.072Z
Modified	2026-04-08T04:08:49.797Z
Severity	6.3 (Medium) 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 CVSS Calculator
Summary	Predictable DNS Transaction IDs Enable Cache Poisoning in Built-in Resolver
Details	

Summary

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.

Workaround

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.

Configuration

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.

Database specific


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


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

Affected ranges

Type	GIT
Repo	https://github.com/erlang/otp
Events	Introduced 07b8f441ca711f9812fad9e9115bab3c3aa92f79 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
