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

Moderate **RaimoNiskanen** published **GHSA-v884-5jg5-whj8** 2 weeks ago

Package

OTP

Affected versions	Patched versions
>= 17.0	26.2.5.19, 27.3.4.10, 28.4.2

kernel (OTP)

>= 3.0	9.2.4.11, 10.2.7.4, 10.6.2

Description

Impact

The Erlang/OTP 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. Together, this makes DNS cache poisoning practical for an attacker who can observe one query or predict the next ID. The design conflicts with RFC 5452 recommendations for mitigating forged DNS answers.

This is because `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 faked DNS responses are possible.

Solution

The documentation is updated to clarify that `inet_res` should only be used in trusted networks and with trusted recursive resolvers.

The implementation is also improved to use strong random DNS transaction IDs and source ports for every DNS transaction. This should give ample protection against brute forcing fake DNS replies, but it still does not protect against, for example, an adversary in the path of the DNS transaction that can observe the random values before faking malicious replies, an attack known as CAPEC-598: DNS Spoofing.

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.

Affected/Unaffected Versions

A version larger than or equal to one of the listed *patched versions* is **unaffected**; *otherwise*, a version that satisfies an expression listed under *affected versions* is **affected**, and if it does not, it is **unaffected**.

The documentation of the new *OTP version scheme* describes how versions should be compared. Note that versions used prior to OTP 17.0, when the new *OTP version scheme* was introduced, are never listed since it is not well defined how to compare those versions.

In the case of this vulnerability, versions prior to OTP 17.0 are likely also affected.

Severity

Moderate 6.3 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	Low
Availability	None
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-28810

Weaknesses

▶ CWE-340

Credits

LuiginoC Reporter