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

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-28810
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 09:16:20 UTC
Updated	2026-04-07 13:20:11 UTC
Description	Generation of Predictable Numbers or Identifiers vulnerability in Erlang/OTP kernel (inet_res, inet_db modules) allows DNS

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000500000 probability, percentile 0.155830000 (date 2026-04-07)

Problem Types: CWE-340 | CWE-340 CWE-340 Generation of Predictable Numbers or Identifiers

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Erlang	OTP	affected 3.0 * otp	Not specified
CNA	Erlang	OTP	affected 17.0 * otp	Not specified
CNA	Erlang	OTP	affected 07b8f441ca711f9812fad9e9115bab3c3aa92f79 * git	Not specified

References

Reference	Source	Link
github.com/erlang/otp/commit/36f23c9d2cc54afe83671dd7343596d7972839a5	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/erlang/otp/commit/dd15e8eb03548c5e55e9915f0e91389ec6bad9fd	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
www.erlang.org/doc/system/versions.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	www.erlang.org
github.com/erlang/otp/commit/b057a9d995017b1be50d6dc02edd52382f3231b8	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/erlang/otp/security/advisories/GHSA-v884-5jg5-whj8	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
osv.dev/vulnerability/EEF-CVE-2026-28810	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
cna.erlef.org/cves/CVE-2026-28810.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Luigino Camastra / Aisle Research (en)

CNA: Raimo Niskanen (en)

Additional Advisory Data

Workarounds

CNA: 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.

There are currently no legacy QID mappings associated with this CVE.