OCSP designated-responder authorization bypass via missing signature verification

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

Summary

CVE	CVE-2026-32144
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 13:16:46 UTC
Updated	2026-04-07 13:20:11 UTC
Description	Improper Certificate Validation vulnerability in Erlang OTP public_key (pubkey_ocsp module) allows OCSP designated-resp

Risk And Classification

Primary CVSS: v4.0 7.6 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

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

Problem Types: CWE-295 | CWE-295 CWE-295 Improper Certificate Validation

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	7.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N
4.0	CNA	CVSS	7.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:L/SI:L/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 1.16 * otp	Not specified
CNA	Erlang	OTP	affected 11.2 * otp	Not specified
CNA	Erlang	OTP	affected 27.0 * otp	Not specified
CNA	Erlang	OTP	affected 601a012837ea0a5c8095bf24223132824177124d * git	Not specified

References

Reference	Source	Link
github.com/erlang/otp/commit/ac7ff528be857c5d35eb29c7f24106e3a16d4891	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/erlang/otp/commit/49033a6d93a5be0ee0dce04e1fb8b4ae7de1e0c0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
www.erlang.org/doc/system/versions.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	www.erlang.org
cna.erlef.org/cves/CVE-2026-32144.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.org
osv.dev/vulnerability/EEF-CVE-2026-32144	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
github.com/erlang/otp/security/advisories/GHSA-gxrm-pf64-99xm	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Igor Morgenstern / Aisle Research (en)

CNA: Jakub Witczak (en)

CNA: Ingela Anderton Andin (en)

Additional Advisory Data

Workarounds

CNA: For SSL users: * Do not enable OCSP validation setting (current default is {stapling, no_staple}) * Use CRL-based revocation checking by setting the {crl_check, true} SSL option instead For applications using public_key:pkix_ocsp_validate/5 directly: * Pass {is_trusted_responder_fun, Fun} option with a function that validates trusted responder certificates * Restrict OCSP responder access to trusted endpoints via network controls (only applicable if you control the OCSP infrastructure)

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