Authentication bypass for certain API calls

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

Summary

CVE	CVE-2026-25660
State	PUBLISHED
Assigner	ERIC
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 14:16:18 UTC
Updated	2026-04-24 14:39:28 UTC
Description	CodeChecker is an analyzer tooling, defect database and viewer extension for the Clang Static Analyzer and Clang Tidy. A

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from 85b1779b-6ecd-4f52-bcc5-73eac4659dcf

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P/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:N/AU:Y/R:U/V:C/RE:M/U:Red

Problem Types: CWE-290 | CWE-863 | CWE-290 CWE-290 Authentication bypass by spoofing | CWE-863 CWE-863 Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
4.0	85b1779b-6ecd-4f52-bcc5-73eac4659dcf	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

ntegrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P/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:N/AU:Y/R:U/V:C/RE:M/U:Red

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ericsson	CodeChecker	affected 6.27.3 python	Not specified

References

Reference	Source	Link	Tag
github.com/Ericsson/codechecker/security/advisories/GHSA-4v9x-cqc5-j645	85b1779b-6ecd-4f52-bcc5-73eac4659dcf	github.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

Vendor Comments And Credit

Discovery Credit

CNA: Scott Tolley (en)

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