Insecure default administrative credentials in AlloyDB for PostgreSQL

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

Summary

CVE	CVE-2026-7428
State	PUBLISHED
Assigner	GoogleCloud
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 10:16:48 UTC
Updated	2026-05-12 15:09:58 UTC
Description	Prior to 2025-11-03, well-intended users of Terraform or REST API for Google Cloud AlloyDB for PostgreSQL could have c

Risk And Classification

Primary CVSS: v4.0 9.2 CRITICAL from f45cbf4e-4146-4068-b7e1-655ffc2c548c

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

EPSS: 0.000410000 probability, percentile 0.124290000 (date 2026-05-12)

Problem Types: CWE-1392 | CWE-1392 CWE-1392 Use of default credentials

Version	Source	Type	Score	Severity	Vector
4.0	f45cbf4e-4146-4068-b7e1-655ffc2c548c	Secondary	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:I
4.0	CNA	CVSS	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:I

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google Cloud	AlloyDB For PostgreSQL	affected 2025-11-03 date	Not specified

References

Reference	Source	Link	Tags
docs.cloud.google.com/alloydb/docs/release-notes	f45cbf4e-4146-4068-b7e1-655ffc2c548c	docs.cloud.google.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Mark Lawrenson (en)

Additional Advisory Data

Solutions

CNA: This vulnerability was patched on November 3, 2025. Impacted instances have been proactively remediated, and no customer action is needed.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report