pgAdmin 4: Unsafe deserialization (CWE-502) in file-backed session manager leads to remote code execution

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

Summary

CVE	CVE-2026-7818
State	PUBLISHED
Assigner	PostgreSQL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 16:17:38 UTC
Updated	2026-05-11 17:16:35 UTC
Description	Deserialization of untrusted data (CWE-502) in pgAdmin 4 FileBackedSessionManager. The session manager performed u

Risk And Classification

Primary CVSS: v4.0 7.3 HIGH from f86ef6dc-4d3a-42ad-8f28-e6d5547a5007

CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/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: 0.002770000 probability, percentile 0.510500000 (date 2026-05-12)

Problem Types: CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
4.0	f86ef6dc-4d3a-42ad-8f28-e6d5547a5007	Secondary	7.3	HIGH	CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H
4.0	CNA	CVSS	7.3	HIGH	CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H
3.1	f86ef6dc-4d3a-42ad-8f28-e6d5547a5007	Secondary	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

None

Privileges Required

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pgadmin.org	PgAdmin 4	affected 9.15 custom	Not specified

References

Reference	Source	Link	Tags
github.com/pgadmin-org/pgadmin4/issues/9901	f86ef6dc-4d3a-42ad-8f28-e6d5547a5007	github.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: Fernando Bortotti (en)

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