



pgAdmin 4: Stored XSS via crafted PostgreSQL object names in Browser Tree and Explain Visualizer

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-7814
State	PUBLISHED
Assigner	PostgreSQL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 16:17:37 UTC
Updated	2026-05-11 18:16:42 UTC
Description	Stored cross-site scripting (XSS) vulnerability in pgAdmin 4 Browser Tree and Explain Visualizer modules. User-controlled I

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from f86ef6dc-4d3a-42ad-8f28-e6d5547a5007

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000270000 probability, percentile 0.076510000 (date 2026-05-12)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	f86ef6dc-4d3a-42ad-8f28-e6d5547a5007	Secondary	4.8	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N
4.0	CNA	CVSS	4.8	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N
3.1	f86ef6dc-4d3a-42ad-8f28-e6d5547a5007	Secondary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/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/MSX:MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pgadmin.org	PgAdmin 4	affected 6.9 9.15 custom	Not specified

References

Reference	Source	Link	Tags
github.com/pgadmin-org/pgadmin4/issues/9865	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	
github.com/pgadmin-org/pgadmin4/pull/9865	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: Fahar Abbas (en)

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

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