



# CVE-2023-5002

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

## Summary

<b>CVE</b>	CVE-2023-5002
<b>State</b>	PUBLIC
<b>Assigner</b>	patrick@puiterwijk.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-22 14:15:00 UTC
<b>Updated</b>	2023-11-07 04:23:00 UTC
<b>Description</b>	A flaw was found in pgAdmin. This issue occurs when the pgAdmin server HTTP API validates the path a user selects to ex

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Application	<a href="#">Pgadmin</a>	<a href="#">Pgadmin</a>	All	All	All	All

## References

Reference	Source	Link
2239164 – (CVE-2023-5002) CVE-2023-5002 pgadmin4: remote code execution by an authenticated user	MISC	<a href="#">bugzilla.r</a>
[SECURITY] Fedora 38 Update: pgadmin4-6.21-3.fc38 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedo</a>
[SECURITY] Fedora 37 Update: pgadmin4-6.19-2.fc37 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedo</a>
Remote command Execution by an Authenticated user in pgAdmin 4 · Issue #6763 · pgadmin-org/pgadmin4 · GitHub	MISC	<a href="#">github.cc</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[284576](#) Fedora Security Update for pgadmin4 (FEDORA-2023-478aa17fa2)

[284577](#) Fedora Security Update for pgadmin4 (FEDORA-2023-8cc61c8b14)

[995372](#) Python (Pip) Security Update for pgadmin4 (GHSA-ghp8-52vx-77j4)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)