VDB-355388 · CVE-2026-5594 · GCVE-100-355388

PREMAI-IO PREMSQL UP TO 0.2.1 FOLLOWUP.PY EVAL RESULT CODE INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	2.45-

Summary

A vulnerability described as critical has been identified in premAI-io premsql up to 0.2.1. Affected by this vulnerability is the function `eval` of the file *premsql/agents/baseline/workers/followup.py*. Such manipulation of the argument *result* leads to code injection. This vulnerability is listed as CVE-2026-5594. The attack may be performed from remote. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in premAI-io premsql up to 0.2.1 and classified as critical. Affected by this issue is the function `eval` of the file *premsql/agents/baseline/workers/followup.py*. The manipulation of the argument `result` with an unknown input leads to a code injection vulnerability. Using CWE to declare the problem leads to CWE-94. The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment. Impacted is confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is handled as CVE-2026-5594. The exploitation is known to be easy. The attack may be launched remotely. Technical details as well as a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1059.

The exploit is available at github.com. It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

See VDB-346382, VDB-347789, VDB-348281 and VDB-349518 for similar entries.

Product

Vendor

- premAI-io

Name

- premsql

Version

- 0.2.0
- 0.2.1

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Code injection
CWE: CWE-94 / CWE-74 / CWE-707
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Programming Language: 🔒
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5594 (🔒)
GCVE (CVE): GCVE-0-2026-5594
GCVE (VulDB): GCVE-100-355388
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 07:17 AM
Changes: 04/05/2026 07:17 AM (57)
Complete: 🔍
Submitter: Goku
Cache ID: 64:6E6:179

Submit

Accepted

- Submit #784462: premsql v0.2.1 Code Injection (by Goku)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa