



premAI-io premsql followup.py eval code injection

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

Summary

CVE	CVE-2026-5594
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-05 19:17:05 UTC
Updated	2026-04-07 13:20:35 UTC
Description	A weakness has been identified in premAI-io premsql up to 0.2.1. Affected is the function eval of the file premsql/agents/bas

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/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: 0.000440000 probability, percentile 0.133460000 (date 2026-04-07)

Problem Types: CWE-74 | CWE-94 | CWE-94 Code Injection | CWE-74 Injection

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	6.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

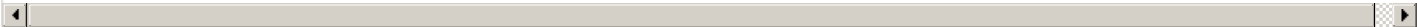
Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R



Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	PremAI-io	Premsql	affected 0.2.0	Not specified
CNA	PremAI-io	Premsql	affected 0.2.1	Not specified

References				
Reference	Source	Link	Tags	
vuldb.com/vuln/355388/cti	cna@vuldb.com	vuldb.com		
github.com/Ka7arotto/cve/blob/main/premsql-rce/poc.py	cna@vuldb.com	github.com		
vuldb.com/vuln/355388	cna@vuldb.com	vuldb.com		
vuldb.com/submit/784462	cna@vuldb.com	vuldb.com		
github.com/Ka7arotto/cve/blob/main/premsql-rce/issue.md	cna@vuldb.com	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: Goku (VulDB User) (en)	
CNA: VulDB CNA Team (en)	

Additional Advisory Data		
Source	Time	Event
CNA	2026-04-05T00:00:00.000Z	Advisory disclosed

CNA	2026-04-05T02:00:00.000Z	VulDB entry created
CNA	2026-04-05T07:17:44.000Z	VulDB entry last update
There are currently no legacy QID mappings associated with this CVE.		

© [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](#)