VDB-355386 · CVE-2026-5587 · GCVE-100-355386

WBBEYOURSELF MAC-SQL UP TO 31A9DF5E0D520BE4769BE57A4B9022E5E34A14F4 REFINER AGENT CORE/AGENTS.PY _EXECUTE_SQL SQL INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	3.05-

Summary

A vulnerability labeled as critical has been found in wbbeyourself MAC-SQL up to 31a9df5e0d520be4769be57a4b9022e5e34a14f4. This impacts the function `_execute_sql` of the file *core/agents.py* of the component *Refiner Agent*. The manipulation results in sql injection. This vulnerability is identified as CVE-2026-5587. The attack can be executed remotely. Additionally, an exploit exists. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as critical, was found in wbbeyourself MAC-SQL up to 31a9df5e0d520be4769be57a4b9022e5e34a14f4. Affected is the function `_execute_sql` of the file *core/agents.py* of the component *Refiner Agent*. The manipulation with an unknown input leads to a sql injection vulnerability. CWE is classifying the issue as CWE-89. The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is traded as CVE-2026-5587. The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known. This vulnerability is assigned to T1505 by the MITRE ATT&CK project.

The exploit is shared for download 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.

Product

Vendor

- wbbeyourself

Name

- MAC-SQL

Version

- 31a9df5e0d520be4769be57a4b9022e5e34a14f4

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: Sql injection
CWE: CWE-89 / CWE-74 / CWE-707
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

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

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

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

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5587 (🔒)
GCVE (CVE): GCVE-0-2026-5587
GCVE (VulDB): GCVE-100-355386
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/04/2026 11:55 PM
Changes: 04/04/2026 11:55 PM (58)
Complete: 🔍
Submitter: Goku
Cache ID: 135:FFF:179

Submit

Accepted

- Submit #784459: MAC-SQL The latest version SQL Injection (by Goku)

Discussion

No comments yet. Languages: en.

Please log in to comment.