VDB-354182 · CVE-2026-5148 · GCVE-100-354182

YUNAIV YUDAO-CLOUD UP TO 2026.01 PAGE TOMAIL SQL INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.3	$0-$5k	1.52

Summary

A vulnerability labeled as critical has been found in YunaiV yudao-cloud up to 2026.01. This issue affects some unknown processing of the file */admin-api/system/mail-log/page*. Such manipulation of the argument *toMail* leads to sql injection. This vulnerability is uniquely identified as CVE-2026-5148. The attack can be launched remotely. Moreover, an exploit is present. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in YunaiV yudao-cloud up to 2026.01 and classified as critical. Affected by this issue is an unknown part of the file */admin-api/system/mail-log/page*. The manipulation of the argument `toMail` with an unknown input leads to a sql injection vulnerability. Using CWE to declare the problem leads to 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. Impacted is confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is handled as CVE-2026-5148. The exploitation is known to be easy. The attack may be launched remotely. Additional levels of successful authentication are required for exploitation. Technical details as well as a public exploit are known. This vulnerability is assigned to T1505 by the MITRE ATT&CK project.

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.

The entries VDB-323645, VDB-323647, VDB-325910 and VDB-338429 are pretty similar.

Product

Type

- Cloud Software

Vendor

- YunaiV

Name

- yudao-cloud

Version

- 2026.01

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 4.7
VulDB Meta Temp Score: 4.3

VulDB Base Score: 4.7
VulDB Temp Score: 4.3
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

03/30/2026		Advisory disclosed
03/30/2026	+0 days	VulDB entry created
03/30/2026	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5148 (🔒)
GCVE (CVE): GCVE-0-2026-5148
GCVE (VulDB): GCVE-100-354182
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/30/2026 03:28 PM
Changes: 03/30/2026 03:28 PM (57)
Complete: 🔍
Submitter: Narcher
Cache ID: 20:51F:179

Submit

Accepted

- Submit #780192: YunaiV yudao-cloud <=v2026.01 SQL Injection (by Narcher)

Discussion

No comments yet. Languages: en.

Please log in to comment.