VDB-355384 · CVE-2026-5585 · GCVE-100-355384

TENCENT AI-INFRA-GUARD 4.0 TASK DETAIL ENDPOINT TASK_MANAGER.GO INFORMATION DISCLOSURE

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.8	$0-$5k	3.29

Summary

A vulnerability categorized as problematic has been discovered in Tencent AI-Infra-Guard 4.0. The impacted element is an unknown function of the file *common/websocket/task_manager.go* of the component *Task Detail Endpoint*. Executing a manipulation can lead to information disclosure. The identification of this vulnerability is CVE-2026-5585. The attack may be launched remotely. Furthermore, there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability classified as problematic was found in Tencent AI-Infra-Guard 4.0. This vulnerability affects an unknown functionality of the file *common/websocket/task_manager.go* of the component *Task Detail Endpoint*. The manipulation with an unknown input leads to a information disclosure vulnerability. The CWE definition for the vulnerability is CWE-200. The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. As an impact it is known to affect confidentiality.

The advisory is shared for download at gist.github.com. This vulnerability was named CVE-2026-5585. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details and also a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1592.

It is possible to download the exploit at gist.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

Type

- Artificial Intelligence Software

Vendor

- Tencent

Name

- AI-Infra-Guard

Version

- 4.0

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 4.8

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Information disclosure
CWE: CWE-200 / CWE-284 / CWE-266
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: gist.github.com
Status: Not defined

CVE: CVE-2026-5585 (🔒)
GCVE (CVE): GCVE-0-2026-5585
GCVE (VulDB): GCVE-100-355384
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/04/2026 11:38 PM
Changes: 04/04/2026 11:38 PM (57)
Complete: 🔍
Submitter: Eric-y
Cache ID: 52:D90:179

Submit

Accepted

- Submit #784198: Tencent AI-Infra-Guard 4.0 Information Disclosure (CWE-200) (by Eric-y)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa