COMMUNITY CONTENT

Home › Submit › 784198

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

Title Tencent AI-Infra-Guard 4.0 Information Disclosure (CWE-200)

Description

Technical Details

A Sensitive Data Exposure vulnerability exists in the [GetTaskDetail](cci:1://file:///root/llm-project-python/AI-Infra-Guard/common/websocket/task_manager.go:1270:0-1357:1) method in [common/websocket/task_manager.go](cci:7://file:///root/llm-project-python/AI-Infra-Guard/common/websocket/task_manager.go:0:0-0:0) of AI-Infra-Guard.

The application fails to mask sensitive API tokens when returning task detail responses. While commit e5582e7 introduced `maskToken()` for the Model List API, the same protection was omitted for the Task Detail endpoint. When [GetTaskDetail](cci:1://file:///root/llm-project-python/AI-Infra-Guard/common/websocket/task_manager.go:1270:0-1357:1) is called, it unmarshals `session.Params` and returns it verbatim, including plaintext model API tokens.

Vulnerable Code

File: common/websocket/task_manager.go
Method: GetTaskDetail
Why: The method unmarshals session.Params containing the raw API token and includes it in the HTTP response without any masking or redaction. The existing maskToken() function used in the Model List API was not applied here.

Reproduction

1. Submit a task via POST /api/v1/app/taskapi/tasks with a known API token in the model configuration.
2. Retrieve the task detail via GET /api/v1/app/tasks/{sessionId}.
3. Observe the plaintext API token in the response JSON under params.model.token.

Impact

- Credential Leak: AI model API keys are exposed in plaintext to any user who can access the task detail endpoint.
- Financial Loss: Stolen API keys can be used to consume paid API quota.

Source https://gist.github.com/YLChen-007/fe4b8341444ad535d167507c2008d4011

User Eric-y (UID 95885)

Submission 03/20/2026 03:48 PM (16 days ago)

Moderation 04/04/2026 11:33 PM (15 days later)

Status Confirmed

VulDB entry VDB-[redacted] [Tencent AI-Infra-Guard 4.0 Task Detail Endpoint task_manager.go information disclosure]

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling

Points 20