August 8, 2026

# GHSL-2024-200_GHSL-2024-201: Zero click RCE in Uptrain - CVE-2025-27771, CVE-2025-27772

Kevin Stubbings

## Coordinated Disclosure Timeline

- 2024-09-05: Issue opened in repo. No response from maintainers.
- 2025-03-10: Uptrain Slack messages suggest project is no longer being maintained.
- 2026-08-10: Pull request opened with suggested fix.

## Summary

The Uptrain dashboard lacks significant authentication, has an open CORS policy, and is vulnerable to a remote code execution vulnerability. Combining these primitives, an attacker can get zero click remote code execution in the context of the Uptrain host by directing an Uptrain user to a specially crafted website.

## Project

Uptrain

## Tested Version

v0.7.1

## Details

### Issue 1: Remote code execution via `/add_prompts` endpoint (`GHSL-2024-200`)

The `/add_prompts` endpoint is vulnerable to remote code execution via the `checks` and `metadata` parameters.

```
@router_public.post("/add_prompts")
async def add_prompts(
    project_id: str = Form(...),
    model: str = Form(...),
    dataset_name: str = Form(...),
    prompt: str = Form(...),
    checks: list = Form(...),
    metadata: str = Form(...),
    prompt_name: str = Form(...),
    data_file: UploadFile = File(...),
    user_id: str = Depends(validate_api_key_public),
    db: Session = Depends(get_db),
    fsspec_fs: t.Any = Depends(get_fsspec_fs),
):
    ## project key would be present in the eval_args.metadata

    # user = db.query(ModelUser).filter_by(id=user_id).first()
    # if user is None:
    #     raise HTTPException(status_code=403, detail="Invalid user name")
    # else:
    #     user_name = user.name

    existing_project = (
        db.query(ModelProject)
        .filter_by(id=project_id)
        .first()
    )

    checks = eval(checks[0])
    checks_1 = []
    metadata = eval(metadata)
```

Any user that has access to Uptrain and a valid authentication method may be able to execute arbitrary code in the context of the host running Uptrain, which in most cases will be the docker container as suggested by the documentation.

This vulnerability was found with the help of the CodeQL Code Injection Query.

### Impact

This issue may lead to `Remote Code Execution`.

## Issue 2: Remote code execution via `/new_run` endpoint (`GHSL-2024-201`)

The `/new_run` endpoint is vulnerable to remote code execution via the `checks` and `metadata` parameters.

```
@router_public.post("/new_run")
async def new_run(
    model: str = Form(...),
    dataset_name: str = Form(...),
    evaluation_name: str = Form(...),
    checks: list = Form(...),
    project_id: str = Form(...),
    data_file: UploadFile = File(...),
    metadata: str = Form(...),
    user_id: str = Depends(validate_api_key_public),
    db: Session = Depends(get_db),
    fsspec_fs: t.Any = Depends(get_fsspec_fs),
):
```

```
    ## project key would be present in the eval_args.metadata

    existing_project = (
        db.query(ModelProject)
        .filter_by(id=project_id)
        .first()
    )

    checks = eval(checks[0])
    checks_1 = []
    metadata = eval(metadata)
```

Any user that has access to Uptrain and a valid authentication method may be able to execute arbitrary code in the context of the host running Uptrain, which in most cases will be the docker container as suggested by the documentation.

This vulnerability was found with the help of the CodeQL Code Injection Query.

**Impact**

This issue may lead to `Remote Code Execution`.

# CVE

- CVE-2025-27771 - GHSL-2024-200
- CVE-2025-27772 - GHSL-2024-201

# Credit

These issues were discovered and reported by GHSL team member @Kwstubbs (Kevin Stubbings).

# Contact

You can contact the GHSL team at `securitylab@github.com`, please include a reference to `GHSL-2024-200` or `GHSL-2024-201` in any communication regarding these issues.

## Platform

- Developer API
- Partners
- Atom
- Electron
- GitHub Desktop

## Support

- Docs
- Community Forum
- Professional Services
- GitHub Skills
- Status
- Contact GitHub

## Company

- About
- Blog
- Careers
- Press
- Inclusion
- Social Impact
- Shop