Bug 2459998 (CVE-2026-6859) - CVE-2026-6859 instructlab: InstructLab: Arbitrary code execution due to hardcoded `trust_remote_code=True`

Keywords: Security ×

Status: NEW

Alias: CVE-2026-6859

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-04-21 07:51 UTC by OSIDB Bzimport

Modified: 2026-04-22 12:59 UTC (History)

CC List: 1 user (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-04-21 07:51:02 UTC Description

```
InstructLab hardcodes trust_remote_code=True in linux_train.py
for all HuggingFace from_pretrained() calls. This enables
arbitrary Python code execution from malicious model
repositories on HuggingFace Hub. Attacker needs only a free
HuggingFace account; victim runs ilab train/download/generate
with the malicious model name.

Upstream notification: security-reporting bounced for external
senders. Filed via Red Hat.
```

Note

You need to log in before you can comment on or make changes to this bug.