



# Instructlab: instructlab: arbitrary code execution due to hardcoded `trust\_remote\_code=true`

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-6859
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-22 14:17:07 UTC
<b>Updated</b>	2026-04-22 21:23:52 UTC
<b>Description</b>	A flaw was found in InstructLab. The `linux_train.py` script hardcodes `trust_remote_code=True` when loading models from

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from secalert@redhat.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**Problem Types:** CWE-829 | CWE-829 Inclusion of Functionality from Untrusted Control Sphere

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux AI RHEL AI 3	Not specified	Not specified

### References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-6859	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Red Hat would like to thank Martin Brodeur (independent security researcher) for reporting this issue. (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-04-15T00:00:00.000Z	Reported to Red Hat.
CNA	2026-04-15T00:00:00.000Z	Made public.

#### Workarounds

**CNA:** To mitigate this issue, only use models from trusted sources when performing `instructlab` operations. Review the origin and integrity of any HuggingFace model before using it with `ilab train/download/generate`. Consider running `instructlab` commands within a sandboxed or isolated environment to limit the potential impact of executing untrusted code.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)