Instructlab: instructlab: arbitrary code execution due to hardcoded `trust_remote_code=true`

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-6859
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:17:07 UTC
Updated	2026-04-22 21:23:52 UTC
Description	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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**