Arbitrary Code Execution via Unsafe torch.load() in Trainer Checkpoint Loading in huggingface/transformers

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

Summary

CVE	CVE-2026-1839
State	PUBLISHED
Assigner	@huntr_ai
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 06:16:41 UTC
Updated	2026-04-07 14:16:18 UTC
Description	A vulnerability in the HuggingFace Transformers library, specifically in the `Trainer` class, allows for arbitrary code executio

Risk And Classification

Primary CVSS: v3.0 6.5 MEDIUM from security@huntr.dev

CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:H

EPSS: 0.000200000 probability, percentile 0.052420000 (date 2026-04-07)

Problem Types: CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.0	security@huntr.dev	Secondary	6.5	MEDIUM	CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:H
3.0	CNA	DECLARED	6.5	MEDIUM	CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:H

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

Low

Availability

High

CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Huggingface	Huggingface/transformers	affected unspecified v5.0.0rc3 custom	Not specified

References

Reference	Source	Link
github.com/huggingface/transformers/commit/03c8082ba4594c9b8d6fe190ca9be...	security@huntr.dev	github.com
huntr.com/bounties/3c77bb97-e493-493d-9a88-c57f5c536485	134c704f-9b21-4f2e-91b3-4a467353bcc0	huntr.com
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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