Safe Mode Bypass in keras-team/keras

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

Summary

CVE	CVE-2026-1462
State	PUBLISHED
Assigner	@huntr_ai
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 15:17:18 UTC
Updated	2026-04-13 15:17:18 UTC
Description	A vulnerability in the `TFSMLayer` class of the `keras` package, version 3.13.0, allows attacker-controlled TensorFlow Save

Risk And Classification

Primary CVSS: v3.0 8.8 HIGH from security@huntr.dev

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

EPSS: 0.000600000 probability, percentile 0.187810000 (date 2026-04-15)

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

Version	Source	Type	Score	Severity	Vector
3.0	security@huntr.dev	Secondary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.0	CNA	DECLARED	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/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	Keras-team	Keras-team/keras	affected unspecified 3.13.2 custom	Not specified

References

Reference	Source	Link	Tags
huntr.com/bounties/7e78d6f1-6977-4300-b595-e81bdbda331c	security@huntr.dev	huntr.com	
github.com/keras-team/keras/commit/b6773d3decaef1b05d8e794458e148cb362f163f	security@huntr.dev	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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