



# Safe Mode Bypass in keras-team/keras

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-1462
<b>State</b>	PUBLISHED
<b>Assigner</b>	@huntr_ai
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-13 15:17:18 UTC
<b>Updated</b>	2026-04-13 15:17:18 UTC
<b>Description</b>	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

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	<a href="#">Keras-team</a>	<a href="#">Keras-team/keras</a>	affected unspecified 3.13.2 custom	Not specified

### References

Reference	Source	Link	Tags
<a href="https://huntr.com/bounties/7e78d6f1-6977-4300-b595-e81bdbda331c">huntr.com/bounties/7e78d6f1-6977-4300-b595-e81bdbda331c</a>	<a href="mailto:security@huntr.dev">security@huntr.dev</a>	<a href="https://huntr.com">huntr.com</a>	
<a href="https://github.com/keras-team/keras/commit/b6773d3decaef1b05d8e794458e148cb362f163f">github.com/keras-team/keras/commit/b6773d3decaef1b05d8e794458e148cb362f163f</a>	<a href="mailto:security@huntr.dev">security@huntr.dev</a>	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, anal

No vendor comments have been submitted for this CVE.

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)