CISA adds exploited GPUStack AI model-serving flaw to its catalogue, fix due 12 November

Source copy kept by wheresthe.ai for the story “CISA adds exploited GPUStack AI model-serving flaw to its catalogue, fix due 12 November” (https://wheresthe.ai/d/us-cisa-adds-exploited-gpustack-ai-model-serving-flaw-to-its-2026-11/).

Source: https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-102895

Text saved 11 Nov 2026 (the page text after its scripts ran in a browser).

SHA-256 of the saved text: 5a2e270cef4b79941bb8a66fbe0800188df274e20d39c798c3e486137dc74c6d

---

Skip to main content

An official website of the United States government

Here’s how you know

STAYING SECURE AT EVENTS NO-COST CYBER SERVICES CYBERSECURITY AWARENESS MONTH KEV CATALOG REPORT A CYBER ISSUE

Search

Topics Spotlight Resources & Tools News & Events Careers About Breadcrumb Home Known Exploited Vulnerabilities Catalog SHARE: Opens in a new window Opens in a new window Opens in a new window Search all Known Exploited Vulnerabilities Catalog Search by keyword, term, or phrase Date Added (optional) Last 30 Days Last 60 Days Last 90 Days Last Year CVE Sort by (optional) Date Added Due Date Vendor/Project A-Z Items per page (optional) 20 - All - Filters Vendor/Project Reset Known Exploited Vulnerabilities Catalog

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework. Learn more about how to use the KEV catalog in your organization.

Are you aware of an actively exploited vulnerability not included in the KEV Catalog? NOMINATE A NEW KEV

The KEV catalog is also available in these formats: CSVJSON PRINT VIEW JSON Schema (updated 09-02-2026) License

Showing 1 to 1 of 1 results GPUSTACK | GPUSTACK CVE-2026-102895 GPUStack Improper Authentication Vulnerability: GPUStack contains an improper authentication vulnerability which could allow unauthenticated administrative access, including user and model changes, persistent administrator API-key creation, disclosure of worker and cloud-provider secrets, and code execution through POST /v2/inference-backends/from-yaml.

Related CWEs: CWE-287| CWE-290| CWE-346

Known To Be Used in Ransomware Campaigns? Unknown Forensic triage required per BOD 26-04: Yes Date Added: 2026-11-09 Due Date: 2026-11-12 Action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA’s BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA’s “Forensics Triage Requirements” (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines. Additional Notes Subscribe to the KEV Catalog Updates

Stay up to date on the latest known exploited vulnerabilities.

SUBSCRIBE NOW Return to top Topics Spotlight Resources & Tools News & Events Careers About Cybersecurity & Infrastructure Security Agency Facebook X LinkedIn YouTube Instagram RSS CISA Central 1-844-Say-CISA contact@cisa.dhs.gov DHS Seal CISA.gov An official website of the U.S. Department of Homeland Security About CISA Budget and Performance DHS.gov FOIA Requests No FEAR Act Office of Inspector General Privacy Policy Subscribe The White House USA.gov Website Feedback