



BentoML has Dockerfile Command Injection via `system_packages` in `bentofile.yaml`

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-33744 |
| State | PUBLISHED |
| Assigner | GitHub_M |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-03-27 01:16:21 UTC |
| Updated | 2026-04-01 15:00:48 UTC |
| Description | BentoML is a Python library for building online serving systems optimized for AI apps and model inference. Prior to 1.4.37, 1 |

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from security-advisories@github.com

CVSS: 3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.000200000 probability, percentile 0.051730000 (date 2026-04-01)

Problem Types: CWE-94 | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection')

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------|-----------|-------|----------|--|
| 3.1 | security-advisories@github.com | Secondary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | CNA | DECLARED | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------|---------|---------|--------|---------|----------|
| Application | Bentoml | Bentoml | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|---------|---------|-------------------|---------------|
| CNA | Bentoml | BentoML | affected < 1.4.37 | Not specified |

References

| Reference | Source | Link | Tags |
|--|--------------------------------|--------------|----------------------|
| github.com/bentoml/BentoML/security/advisories/GHSA-jfjg-vc52-wqvf | security-advisories@github.com | github.com | Exploit, Mitigation, |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

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.

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