Trivy ecosystem supply chain briefly compromised

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-33634
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 22:16:31 UTC
Updated	2026-03-30 18:50:38 UTC
Description	Trivy is a security scanner. On March 19, 2026, a threat actor used compromised credentials to publish a malicious Trivy v0

Risk And Classification

Primary CVSS: v4.0 9.4 CRITICAL from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.211530000 probability, percentile 0.956250000 (date 2026-04-01)

CISA KEV: Listed on 2026-03-26; due 2026-04-09; ransomware use Unknown

Problem Types: CWE-506 | CWE-506 CWE-506: Embedded Malicious Code

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	9.4	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/
4.0	CNA	DECLARED	9.4	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CISA Known Exploited Vulnerability

Vendor	Aquasecurity
Product	Trivy
Name	Aquasecurity Trivy Embedded Malicious Code Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Notes	This vulnerability involves a supply-chain compromise in a product that may be used across multiple products and environments. Additional vendor-provided guidance must be followed to ensure full remediation. For more information, please see: https://github.com/advisories/GHSA-69fq-xp46-6x23 ; https://nvd.nist.gov/vuln/detail/CVE-2026-33634

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aquasec	Setup-trivy	All	All	All	All
Application	Aquasec	Trivy	0.69.4	All	All	All
Application	Aquasec	Trivy Action	All	All	All	All
Application	Litellm	Litellm	1.82.7	All	All	All
Application	Litellm	Litellm	1.82.8	All	All	All
Application	Telnyx	Telnyx	4.87.1	All	All	All
Application	Telnyx	Telnyx	4.87.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Aquasecurity	Setup-trivy	affected < 0.2.6	Not specified
CNA	Aquasecurity	Trivy-action	affected < 0.35.0	Not specified
CNA	Aquasecurity	Trivy	affected = 0.69.4	Not specified
CNA	BerriAI	LiteLLM	affected >= 1.82.7, <= 1.82.8	Not specified
CNA	Team-telnyx	Telnyx	affected >= 4.87.1, <= 4.87.2	Not specified

References

Reference	Source	Link
inspector.pypi.io/project/litellm/1.82.8/packages/f6/2c/731b614e6cee0bca1e010a3...	security-advisories@github.com	inspector.p
github.com/aquasecurity/trivy/security/advisories/GHSA-69fq-xp46-6x23	security-advisories@github.com	github.com
github.com/BerriAI/litellm/issues/24518	security-advisories@github.com	github.com
rosesecurity.dev/2026/03/20/typosquatting-trivy.html	134c704f-9b21-4f2e-91b3-4a467353bcc0	rosesecurit
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.g
github.com/aquasecurity/trivy/discussions/10425	security-advisories@github.com	github.com
github.com/pypa/advisory-database/tree/main/vulns/litellm/PYSEC-2026-2.yaml	security-advisories@github.com	github.com
futuresearch.ai/blog/litellm-pypi-supply-chain-attack	security-advisories@github.com	futuresearc
inspector.pypi.io/project/litellm/1.82.7/packages/79/5f/b6998d42c6ccd32d36e1266...	security-advisories@github.com	inspector.p
www.wiz.io/blog/teampcp-attack-kics-github-action	security-advisories@github.com	www.wiz.io
github.com/team-telnyx/telnyx-python/security/advisories/GHSA-955r-262c-...	security-advisories@github.com	github.com
www.microsoft.com/en-us/security/blog/2026/03/24/detecting-investigating-defend...	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.micro
github.com/BerriAI/litellm/issues/24518	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com

docs.litellm.ai/blog/security-update-march-2026	security-advisories@github.com	docs.litellm
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.g

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2026-03-26T00:00:00.000Z	CVE-2026-33634 added to CISA KEV

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