Giskard has a Regular Expression Denial of Service (ReDoS) in RegexMatching Check

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

Summary

CVE	CVE-2026-40319
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 18:16:32 UTC
Updated	2026-04-17 19:01:56 UTC
Description	Giskard is an open-source testing framework for AI models. In versions prior to 1.0.2b1, the RegexMatching check passes a

Risk And Classification

Primary CVSS: v4.0 1 LOW from security-advisories@github.com

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:L/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: 0.000150000 probability, percentile 0.029270000 (date 2026-04-20)

Problem Types: CWE-1333 | CWE-1333 CWE-1333: Inefficient Regular Expression Complexity

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	1	LOW	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:L/SC:N/SI
4.0	CNA	DECLARED	1	LOW	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:L/SC:N/SI

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

Passive

Passive

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

Low

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:L/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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Giskard-AI	Giskard-oss	affected < 1.0.2b1	Not specified

References

Reference	Source	Link	Tags
github.com/Giskard-AI/giskard-oss/security/advisories/GHSA-rq2q-4r55-9877	security-advisories@github.com	github.com	
github.com/Giskard-AI/giskard-oss/releases/tag/giskard-checks%2Fv1.0.2b1	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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