Regular Expression Denial of Service (ReDoS) in RegexMatching Check

Low **mattbit** published **GHSA-rq2q-4r55-9877** 4 days ago

Package

giskard-checks (pip)

Affected versions

<= 1.0.1b1

Patched versions

1.0.2b1

Description

Summary

The RegexMatching check in the `giskard-checks` package passes a user-supplied regular expression pattern directly to Python's re.search() without any timeout, complexity guard, or pattern validation. An attacker who can control the regex pattern or the text being matched can craft inputs that trigger catastrophic backtracking in the regex engine, causing the process to hang indefinitely and denying service to all other operations.

`giskard-checks` is a local developer testing library. Check definitions, including the pattern parameter, are provided in application code or configuration files and executed locally. Exploitation requires write access to a check definition and subsequent execution of the test suite. The absence of a regex timeout could cause availability issues in automated environments such as CI/CD pipelines.

Affected component

`text_matching.py`, line 457: `re.search(pattern, text)`

Severity

Low CVSS 4 Base Score: 1.0

`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`

Weakness

CWE-1333: Inefficient Regular Expression Complexity

Remediation

Upgrade to `giskard-checks` >= 1.0.2b1.

Credit

We thank **@dhabaleshwar** for identifying the missing timeout on regex evaluation.

Severity

Low 1.0 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Local
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	Low
User interaction	Passive
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	Low
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	Low

Learn more about base metrics

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

CVE ID

CVE-2026-40319

Weaknesses

▶ CWE-1333

Credits

 **dhabaleshwar** Reporter