# Unsandboxed Jinja2 Template Rendering in ConformityCheck

Moderate **mattbit** published **GHSA-7xjm-g8f4-rp26** 4 days ago

**Package**

**giskard-checks** (pip)

**Affected versions**

<= 1.0.1b1

**Patched versions**

1.0.2b1

**Description**

## Summary

The `ConformityCheck` class in `giskard-checks` rendered the `rule` parameter through Jinja2's default `Template()` constructor. Because the `rule` string is silently interpreted as a Jinja2 template, a developer may not realize that template expressions embedded in rule definitions are evaluated at runtime. In a scenario where check definitions are loaded from an untrusted source (e.g. a shared project file or externally contributed configuration), this could lead to arbitrary code execution.

`giskard-checks` is a local developer testing library with no network-facing service. Check definitions, including the `rule` parameter, are provided in application code or project configuration files and executed locally. Exploitation requires write access to a check definition and subsequent execution of the test suite by a developer.

However, the implicit template evaluation of the `rule` parameter is not obvious from the API surface. This hidden behavior increases the likelihood of a developer inadvertently passing untrusted input to it when integrating the library into a larger system.

## Affected Component

`conformity.py`, line 59:

```
from jinja2 import Template
...
```

```
formatted_rule = Template(self.rule).render(trace=trace)
```

## Affected Versions

`giskard-checks` < 1.0.2b1

## Patched Version

`giskard-checks` >= **1.0.2b1** (template parsing removed from rule evaluation entirely)

## Severity

**Medium** — CVSS 4.0 Base Score: **5.4**

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

## Weakness

CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine

## Remediation

Upgrade to `giskard-checks` >= 1.0.2b1. The template rendering has been removed from rule evaluation.

## Credit

We thank **@dhabaleshwar** for identifying the unsandboxed template usage.

**Severity**

Moderate 5.4 / 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 | High |
| Integrity | High |
| Availability | High |
| **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:H/VI:H/VA:H/SC:N/SI:N/SA:L

### CVE ID

CVE-2026-40320

### Weaknesses

▶ CWE-1336

### Credits

**dhabaleshwar** Reporter