# Authentication/Authorization bypasses

High **cescoffier** published **GHSA-rc95-pcm8-65v9** yesterday

**Package**

**io.quarkus:quarkus-vertx-http** (Maven)

**Affected versions**

<3.20.6, <3.27.3, <3.33.1, <3.35.1

**Patched versions**

3.35.1.1. 3.27.3.1, 3.20.6.1, 3.33.1.1, 3.35.2, 3.34.7

## Description

Quarkus version 3.32.4 is vulnerable to an authorization bypass issue (GHSL-2026-099), in which semicolons (matrix parameters) in HTTP requests can be used to bypass security constraints, potentially allowing unauthorized access to protected resources.

Unauthenticated or lower-privileged users can bypass HTTP path-based authorization policies by appending a semicolon (`;`) and arbitrary text to the request URL. The vulnerability arises from a path-normalization inconsistency: Quarkus's security layer performs authorization checks on the raw URL path (which preserves matrix parameters), whereas RESTEasy Reactive's routing layer strips matrix parameters before matching endpoints. This allows requests like `/api/admin;anything` to bypass policies protecting `/api/admin` while still routing to the protected endpoint.

### Impact

This issue may lead to Authentication/Authorization bypasses.

### Credits

This issue was discovered with the GitHub Security Lab Taskflow Agent and manually verified by GHSL team members @p- (Peter Stöckli) and @m-y-mo (Man Yue Mo).

**Severity**

High 8.2 / 10

**CVSS v3 base metrics**

| | |
|---|---|
| Attack vector | Network |
| Attack complexity | Low |
| Privileges required | None |
| User interaction | None |
| Scope | Unchanged |
| Confidentiality | High |
| Integrity | Low |
| Availability | None |

Learn more about base metrics

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

**CVE ID**

CVE-2026-39852

**Weaknesses**

No CWEs

**Credits**

 **p-** Reporter