



# CVE-2023-4853

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-4853
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-20 10:15:00 UTC
<b>Updated</b>	2023-12-05 22:15:00 UTC
<b>Description</b>	A flaw was found in Quarkus where HTTP security policies are not sanitizing certain character permutations correctly when

## Risk And Classification

### Problem Types: CWE-863

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Quarkus</a>	<a href="#">Quarkus</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Build Of Optaplanner</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Build Of Quarkus</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Decision Manager</a>	7.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Integration Camel K</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Integration Camel Quarkus</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Integration Service Registry</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Middleware</a>	1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Serverless</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Serverless</a>	1.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Process Automation Manager</a>	7.0	All	All	All

## References

Reference	Source	Link
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
RHSB-2023-002 Quarkus Security Policy Bypass - Quarkus - (CVE-2023-4853) - Red Hat Customer Portal	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>

Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
RHSA-2023:7653		<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
cve-details	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
2238034 – (CVE-2023-4853) CVE-2023-4853 quarkus: HTTP security policy bypass	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
Red Hat	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[995376](#) Java (Maven) Security Update for io.quarkus:quarkus-csrf-reactive (GHSA-4f4r-wgv2-jjvg)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)