



CVE-2023-0044

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-0044
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-23 20:15:00 UTC
Updated	2023-03-03 15:58:00 UTC
Description	If the Quarkus Form Authentication session cookie Path attribute is set to `^` then a cross-site attack may be initiated which

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quarkus	Quarkus	All	All	All	All
Application	Redhat	Build Of Quarkus	-	All	All	All

References

Reference

Red Hat Customer Portal - Access to 24x7 support and knowledge

2158081 – (CVE-2023-0044) CVE-2023-0044 quarkus-vertx-http: a cross-site attack may be initiated which might lead to the Information Disc

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report