



CVE-2023-1584

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

Summary

CVE	CVE-2023-1584
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-04 11:15:00 UTC
Updated	2023-11-07 04:04:00 UTC
Description	A flaw was found in Quarkus. Quarkus OIDC can leak both ID and access tokens in the authorization code flow when an in

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quarkus	Quarkus	All	All	All	All

References

Reference	Source	Link
cve-details	MISC	access.
Red Hat	MISC	access.
Encrypt OIDC session cookie value by default by sberyozkin · Pull Request #32192 · quarkusio/quarkus · GitHub	MISC	github.c
2.13: Encrypt OIDC session cookie value by default by sberyozkin · Pull Request #33414 · quarkusio/quarkus · GitHub	MISC	github.c
2180886 – (CVE-2023-1584) CVE-2023-1584 quarkus-oidc: ID and access tokens leak via the authorization code flow	MISC	bugzilla
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

995501 Java (Maven) Security Update for io.quarkus:quarkus-oidc (GHSA-6hc9-cf8x-hf83)

© [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](#) 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](#)