Io.quarkus:quarkus-resteasy: memory leak in quarkus resteasy classic when client requests timeout

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-1634
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-02-26 17:15:22 UTC
Updated	2026-04-20 19:16:08 UTC
Description	A flaw was found in the quarkus-resteasy extension, which causes memory leaks when client requests with low timeouts ar

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from secalert@redhat.com

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

EPSS: 0.004620000 probability, percentile 0.642850000 (date 2026-04-22)

Problem Types: CWE-401 | CWE-401 Missing Release of Memory after Effective Lifetime

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Apache Camel 4.8 For Quarkus 3.15	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Quarkus 3.15.3.SP1	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Quarkus 3.8.6.SP3	Not specified	Not specified
CNA	Red Hat	Streams For Apache Kafka 2.9.1	Not specified	Not specified
CNA	Red Hat	Streams For Apache Kafka 3.0.0	Not specified	Not specified
CNA	Red Hat	Streams For Apache Kafka 3.1.0	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2025:1884	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:23417	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:2067	secalert@redhat.com	access.redhat.com	
github.com/quarkusio/quarkus/issues/46412	secalert@redhat.com	github.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
github.com/quarkusio/quarkus/pull/46419	secalert@redhat.com	github.com	
access.redhat.com/errata/RHSA-2025:12511	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:1885	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:9922	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2025-1634	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-02-24T14:17:31.237Z	Reported to Red Hat.
CNA	2025-02-24T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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