



CVE-2021-4178

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

Summary

CVE	CVE-2021-4178
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-24 16:15:00 UTC
Updated	2022-10-04 17:55:00 UTC
Description	A arbitrary code execution flaw was found in the Fabric 8 Kubernetes client affecting versions 5.0.0-beta-1 and above. Due

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	A-mq Streams	2.0.1	All	All	All
Application	Redhat	Build Of Quarkus	2.2.5	All	All	All
Application	Redhat	Descision Manager	7.0	All	All	All
Application	Redhat	Fabric8-kubernetes	All	All	All	All
Application	Redhat	Fabric8-kubernetes	5.0.0	beta1	All	All
Application	Redhat	Fabric8-kubernetes	5.8.0	All	All	All
Application	Redhat	Fuse	7.11	All	All	All
Application	Redhat	Integration Camel K	-	All	All	All
Application	Redhat	Integration Camel Quarkus	2.2.1	All	All	All
Application	Redhat	Openshift Application Runtimes	-	All	All	All
Application	Redhat	Process Automation	7.0	All	All	All

References

Reference	Source	Link
Security issue in kubernetes-client · Issue #3653 · fabric8io/kubernetes-client · GitHub	MISC	github.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
fabric8 kubernetes-client vulnerable · CVE-2021-4178 · GitHub Advisory Database · GitHub	MISC	github.com

2034388 – (CVE-2021-4178) CVE-2021-4178 kubernetes-client: Insecure deserialization in unmarshalYaml method	MISC	bugzilla.re
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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

© [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](#)