



CVE-2021-3495

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

Summary

CVE	CVE-2021-3495
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-01 14:15:00 UTC
Updated	2021-06-14 15:13:00 UTC
Description	An incorrect access control flaw was found in the kiali-operator in versions before 1.33.0 and before 1.24.7. This flaw allows

Risk And Classification

Problem Types: CWE-281

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netlify	Kiali-operator	All	All	All	All
Application	Redhat	Openshift Service Mesh	1.0	All	All	All
Application	Redhat	Openshift Service Mesh	2.0	All	All	All

References

Reference	Source	Link
1947361 – (CVE-2021-3495) CVE-2021-3495 kiali/kiali-operator: can deploy specified image to any namespace	MISC	bugzilla.redha
Kiali: Service mesh observability and configuration	MISC	kiali.io
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982243 Go (go) Security Update for github.com/kiali/kiali (GHSA-mv55-23xp-3wp8)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)