



CVE-2020-1764

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-1764
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-26 13:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	A hard-coded cryptographic key vulnerability in the default configuration file was found in Kiali, all versions prior to 1.15.1. A

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kiali	Kiali	All	All	All	All
Application	Kiali	Kiali	All	All	All	All
Application	Redhat	Openshift Service Mesh	1.0	All	All	All
Application	Redhat	Openshift Service Mesh	1.0	All	All	All

References

Reference	Source	Link	Tags
Kiali: Service mesh observability and configuration	MISC	kiali.io	Exploit, Mitigati
1810383 – (CVE-2020-1764) CVE-2020-1764 kiali: JWT cookie uses default signing key	CONFIRM	bugzilla.redhat.com	Issue Tracking,
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982561](#) Go (go) Security Update for github.com/kiali/kiali/config (GHSA-64rh-r86q-75ff)

© [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](#)