CVE-2020-1764

MITRE | NVD | CVE.ORG | Print: PDF

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, analy

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)