# CVE-2020-8566

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-8566 |
| **State** | PUBLIC |
| **Assigner** | security@kubernetes.io |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-12-07 22:15:00 UTC |
| **Updated** | 2021-03-29 19:30:00 UTC |
| **Description** | In Kubernetes clusters using Ceph RBD as a storage provisioner, with logging level of at least 4, Ceph RBD admin secrets |

## Risk And Classification

**Problem Types:** CWE-532

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Kubernetes | Kubernetes | All | All | All | All |
| Application | Kubernetes | Kubernetes | All | All | All | All |

## References

| Reference | Source |
|---|---|
| [Security Advisory] Multiple secret leaks when verbose logging is enabled | MLIST |
| December 2020 Kubernetes Vulnerabilities in NetApp Products \| NetApp Product Security | CONFIRM |
| CVE-2020-8566: Ceph RBD adminSecrets exposed in logs when loglevel >= 4 · Issue #95624 · kubernetes/kubernetes · GitHub | CONFIRM |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Kaizhe Huang (derek0405)

## Legacy QID Mappings

377847 Kubernetes Ceph RBD Admin Secrets exposed Vulnerability

770064 Red Hat OpenShift Container Platform 4.7.0 Packages and Security Update (RHSA-2020:5634)

900232 CBL-Mariner Linux Security Update for kubernetes 1.18.10