



CVE-2021-3636

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

Summary

CVE	CVE-2021-3636
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-30 20:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	It was found in OpenShift, before version 4.8, that the generated certificate for the in-cluster Service CA, incorrectly include

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openshift	All	All	All	All

References

Reference	Source	Link
1978621 – (CVE-2021-3636) CVE-2021-3636 openshift: Injected service-ca.crt incorrectly contains additional internal CAs	MISC	bug
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[239525](#) Red Hat Update for OpenShift Container Platform 4.8.2 (RHSA-2021:2437)

[375759](#) Putty Multiple Security Vulnerabilities

[375787](#) Nagios XI Multiple Vulnerabilities

[770074](#) Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:2437)

[770111](#) Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-2437)

© [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](#)