



CVE-2022-0759

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

Summary

CVE	CVE-2022-0759
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-25 19:15:00 UTC
Updated	2022-04-07 19:13:00 UTC
Description	A flaw was found in all versions of kubeclient up to (but not including) v4.9.3, the Ruby client for Kubernetes REST API, in t

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

- [`Config` ignores `insecure-skip-tls-verify` field · Issue #555 · ManageIQ/kubeclient · GitHub](#)
- [VULNERABILITY: `Config` defaults to `VERIFY_NONE` when kubeconfig doesn't specify custom CA · Issue #554 · ManageIQ/kubeclient · Git](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [182715](#) Debian Security Update for ruby-kubeclient (CVE-2022-0759)
- [242347](#) Red Hat Update for Satellite 6.14 (RHSA-2023:6818)
- [961065](#) Rocky Linux Security Update for Satellite (RLSA-2023:6818)

© [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](#)