



# CVE-2021-20319

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-20319
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-04 18:15:00 UTC
<b>Updated</b>	2022-03-11 15:37:00 UTC
<b>Description</b>	An improper signature verification vulnerability was found in coreos-installer. A specially crafted gzip installation image can

## Risk And Classification

**Problem Types:** CWE-347

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Coreos-installer	All	All	All	All

## References

### Reference

- [coreos-installer < 0.10.1 improperly verifies GPG signature when decompressing gzipped artifact · Advisory · coreos/coreos-installer · GitHub](#)
- [\[release-0.10\] io: check for EOF when decoding a gzip stream \(CVE-2021-20319\) by bgilbert · Pull Request #659 · coreos/coreos-installer · GitHub](#)
- [2011862 – \(CVE-2021-20319\) CVE-2021-20319 coreos-installer: incorrect signature verification on gzip-compressed install images](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[239734](#) Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2021:3934)

[239744](#) Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:3926)

[239745](#) Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021:3930)

<a href="#">239779</a> Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:4008)
<a href="#">282001</a> Fedora Security Update for rust (FEDORA-2021-449a2bdaf3)
<a href="#">282002</a> Fedora Security Update for rust (FEDORA-2021-3d52eb54ca)
<a href="#">770084</a> Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2021:3934)
<a href="#">770085</a> Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:3926)
<a href="#">770086</a> Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021:3930)
<a href="#">770087</a> Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:4008)
<a href="#">770095</a> Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-3930)
<a href="#">770100</a> Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021-4008)
<a href="#">770104</a> Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-3926)
<a href="#">770110</a> Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2021-3934)

© [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](#)