



# CVE-2022-1706

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

## Summary

<b>CVE</b>	CVE-2022-1706
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-05-17 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:42:00 UTC
<b>Description</b>	A vulnerability was found in Ignition where ignition configs are accessible from unprivileged containers in VMs running on V

## Risk And Classification

**Problem Types:** CWE-863

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ignition</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.0	All	All	All

## References

Reference
<a href="#">Merge pull request #1350 from bgilbert/userdata · coreos/ignition@4b70b44 · GitHub</a>
<a href="#">[SECURITY] Fedora 34 Update: ignition-2.14.0-1.fc34 - package-announce - Fedora Mailing-Lists</a>
<a href="#">Delete userdata from VirtualBox/VMware after Ignition completes by bgilbert · Pull Request #1350 · coreos/ignition · GitHub</a>
<a href="#">[SECURITY] Fedora 36 Update: ignition-2.14.0-1.fc36 - package-announce - Fedora Mailing-Lists</a>
<a href="#">Consider deleting userdata from provider after Ignition completes · Issue #1315 · coreos/ignition · GitHub</a>
<a href="#">[SECURITY] Fedora 35 Update: ignition-2.14.0-1.fc35 - package-announce - Fedora Mailing-Lists</a>
<a href="#">[SECURITY] Fedora 36 Update: ignition-2.14.0-1.fc36 - package-announce - Fedora Mailing-Lists</a>
<a href="#">Security when using vmware to store the ignition config? · Issue #1300 · coreos/ignition · GitHub</a>

[SECURITY] Fedora 35 Update: ignition-2.14.0-1.fc35 - package-announce - Fedora Mailing-Lists

2082274 – (CVE-2022-1706) CVE-2022-1706 ignition: configs are accessible from unprivileged containers in VMs running on VMware product

[SECURITY] Fedora 34 Update: ignition-2.14.0-1.fc34 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[160290](#) Oracle Enterprise Linux Security Update for ignition (ELSA-2022-8126)

[183362](#) Debian Security Update for ignition (CVE-2022-1706)

[240607](#) Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2022:5068)

[240887](#) Red Hat Update for ignition security (RHSA-2022:8126)

[282762](#) Fedora Security Update for ignition (FEDORA-2022-7846cac830)

[282763](#) Fedora Security Update for ignition (FEDORA-2022-393948cc9e)

[282764](#) Fedora Security Update for ignition (FEDORA-2022-5df5dc8ec5)

[752492](#) SUSE Enterprise Linux Security Update for systemd-presets-common-SUSE (SUSE-SU-2022:2866-1)

[770161](#) Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:5068)

[940814](#) AlmaLinux Security Update for ignition (ALSA-2022:8126)

[960570](#) Rocky Linux Security Update for ignition (RLSA-2022:8126)

© [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](#)**