



CVE-2014-9356

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

Summary

CVE	CVE-2014-9356
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-02 18:15:00 UTC
Updated	2019-12-11 20:30:00 UTC
Description	Path traversal vulnerability in Docker before 1.3.3 allows remote attackers to write to arbitrary files and bypass a container p

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Docker	Docker	All	All	All	All
Application	Docker	Docker	All	All	All	All

References

Reference	Source	Link	Tags
SecurityFocus	BUGTRAQ	www.securityfocus.com	Brok
Bug 1172761 – CVE-2014-9356 docker: Path traversal during processing of absolute symlinks	MISC	bugzilla.redhat.com	Thir
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[900005](#) CBL-Mariner Linux Security Update for moby-buildx 0.4.1

[902872](#) Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (4414)

[982541](#) Go (go) Security Update for github.com/fsouza/go-dockerclient (GHSA-vj3f-3286-r4pf)

© [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](#)