



CVE-2015-3631

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

Summary

CVE	CVE-2015-3631
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-18 15:59:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	Docker Engine before 1.6.1 allows local users to set arbitrary Linux Security Modules (LSM) and docker_t policies via an im

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
openSUSE-SU-2015:0905-1: moderate: Security update for docker	SUSE	lists.opensuse.org	
Google Grupper		groups.google.com	
Full Disclosure: Docker 1.6.1 - Security Advisory [150507]	FULLDISC	seclists.org	
Docker Privilege Escalation / Information Disclosure ≈ Packet Storm	MISC	packetstormsecurity.com	
Google Grupper	CONFIRM	groups.google.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

900005 CBL-Mariner Linux Security Update for moby-buildx 0.4.1

903669 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (4418)

© [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](#)