



CVE-2018-10892

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

Summary

CVE	CVE-2018-10892
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-06 16:29:00 UTC
Updated	2023-02-12 23:31:00 UTC
Description	The default OCI linux spec in oci/defaults[_linux].go in Docker/Moby from 1.11 to current does not block /proc/acpi pathnam

Risk And Classification

Problem Types: CWE-250

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
Application	Mobyproject	Moby	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Application	Redhat	Openstack	12	All	All	All
Application	Redhat	Openstack	12	All	All	All

References

Reference	Source	Link
CVE-2018-10892 - Red Hat Customer Portal	MISC	access.redhat.c

1598581 – (CVE-2018-10892) CVE-2018-10892 docker: container breakout without selinux in enforcing mode	MISC	bugzilla.redhat.c
Red Hat Customer Portal	REDHAT	access.redhat.c
[security-announce] openSUSE-SU-2019:2021-1: important: Security update	SUSE	lists.opensuse.c
Red Hat Customer Portal	REDHAT	access.redhat.c
Red Hat Customer Portal	REDHAT	access.redhat.c
1598581 – (CVE-2018-10892) CVE-2018-10892 docker: container breakout without selinux in enforcing mode	CONFIRM	bugzilla.redhat.c
Add /proc/acpi to masked paths by runcom · Pull Request #37404 · moby/moby · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[353053](#) Amazon Linux Security Advisory for docker : ALAS2NITRO-ENCLAVES-2021-005

[353066](#) Amazon Linux Security Advisory for docker : ALAS2DOCKER-2021-005

© [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](#)