



CVE-2021-33636

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

Summary

CVE	CVE-2021-33636
State	PUBLIC
Assigner	securities@openeuler.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-29 08:15:00 UTC
Updated	2023-11-08 14:36:00 UTC
Description	When the isula load command is used to load malicious images, attackers can execute arbitrary code.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openeuler	Isula	2.0.18-10	All	All	All
Application	Openeuler	Isula	2.0.8-20210518.144540	All	All	All
Application	Openeuler	Isula	2.1.2	All	All	All

References

Reference
add bind mount file lock · Pull Request !627 · src-openEuler/iSulad - Gitee.com
安全公告详情
adaptation modification for fixing loading of nsswitch based config inside chroot under glibc · Pull Request !600 · src-openEuler/iSulad - Gitee.com
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[673638](#) EulerOS Security Update for isulad (EulerOS-SA-2023-3335)

[673712](#) EulerOS Security Update for isulad (EulerOS-SA-2023-3246)

673719 EulerOS Security Update for isulad (EulerOS-SA-2023-3303)
673827 EulerOS Security Update for isulad (EulerOS-SA-2023-3274)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)