CVE-2022-31647

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-31647
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-27 20:15:00 UTC
Updated	2023-05-09 15:30:00 UTC
Description	Docker Desktop before 4.6.0 on Windows allows attackers to delete any file through the hyperv/destroy dockerBackendV2 .

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Breaking Docker Named Pipes SYSTEMatically: Docker Desktop Privilege Escalation – Part 2	MISC	www.cyberark.com	
Docker Desktop release notes | Docker Documentation	MISC	docs.docker.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**