



CVE-2021-32847

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

Summary

CVE	CVE-2021-32847
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-20 17:15:00 UTC
Updated	2023-03-01 18:03:00 UTC
Description	HyperKit is a toolkit for embedding hypervisor capabilities in an application. In versions 0.20210107 and prior, a malicious g

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mobyproject	Hyperkit	All	All	All	All

References

Reference	Source
hyperkit/pci_virtio_block.c at 2f061e447e1435cdf1b9eda364cea6414f2c606b · moby/hyperkit · GitHub	MISC
GHSL-2021-058: Disclosure of the host memory into the virtualized guest in hyperkit - CVE-2021-32847 GitHub Security Lab	CONFIRM
Fix assertion turned into assignment · moby/hyperkit@cf60095 · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#)