



CVE-2020-7628

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

Summary

CVE	CVE-2020-7628
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-02 22:15:00 UTC
Updated	2022-04-22 19:07:00 UTC
Description	umount through 1.1.6 is vulnerable to Command Injection. The argument device can be controlled by users without any sar

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Install-package Project	Install-package	-	All	All	All
Application	Install-package Project	Install-package	-	All	All	All
Application	Umount Project	Umount	All	All	All	All

References

Reference	Source	Link	Tags
Command Injection in umount Snyk	MISC	snyk.io	Third Party Advisory
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

[981898](#) Nodejs (npm) Security Update for umount (GHSA-6q48-vjq2-mwcj)

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](#)