



CVE-2020-16121

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

Summary

CVE	CVE-2020-16121
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-07 04:15:00 UTC
Updated	2020-11-18 14:30:00 UTC
Description	PackageKit provided detailed error messages to unprivileged callers that exposed information about file presence and mime

Risk And Classification

Problem Types: CWE-209

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Application	Packagekit Project	Packagekit	-	All	All	All
Application	Packagekit Project	Packagekit	-	All	All	All

References

Reference	Source	Link
Bug #1888887 "Reading local files as root leads to sensitive inf..." : Bugs : packagekit package : Ubuntu	CONFIRM	bugs.launchpad.net
The story of three CVE's in Ubuntu Desktop - EYE	MISC	www.eyecontrol.nl
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Vaisha Bernard

Legacy QID Mappings

750458 OpenSUSE Security Update for PackageKit (openSUSE-SU-2020:2344-1)

750480 OpenSUSE Security Update for PackageKit (openSUSE-SU-2020:2292-1)

© [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](#)