



CVE-2018-10380

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

Summary

CVE	CVE-2018-10380
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-08 12:29:00 UTC
Updated	2018-06-12 18:32:00 UTC
Description	kwallet-pam in KDE KWallet before 5.12.6 allows local users to obtain ownership of arbitrary files via a symlink attack.

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Kde	Plasma	All	All	All	All
Application	Kde	Plasma	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All

References

Reference	Source	Link
Move socket creation to unprivileged codepath (01d4143f) · Commits · Plasma / KWallet PAM Integration · GitLab	CONFIRM	commits.kde
Move salt creation to an unprivileged process (2134dec8) · Commits · Plasma / KWallet PAM Integration · GitLab	CONFIRM	commits.kde
Bug 1090863 – VUL-0: CVE-2018-10380: pam_kwallet: Local root vulnerability	CONFIRM	bugzilla.suse
Move salt creation to an unprivileged process (99abc7fd) · Commits · Plasma / KWallet PAM Integration · GitLab	CONFIRM	commits.kde
Move socket creation to unprivileged codepath (802f305d) · Commits · Plasma / KWallet PAM Integration · GitLab	CONFIRM	commits.kde
www.kde.org/info/security/advisory-20180503-1.txt	CONFIRM	www.kde.org
Debian Security Information: DSA-4200-1 kwallet-pam	DEBIAN	www.debian

Debian -- Security information -- DSA-4200-1 kernel-pam	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
There are currently no legacy QID mappings associated with this CVE.		

© [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