



# CVE-2019-6133

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

## Summary

<b>CVE</b>	CVE-2019-6133
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-01-11 14:29:00 UTC
<b>Updated</b>	2020-08-24 17:37:00 UTC
<b>Description</b>	In PolicyKit (aka polkit) 0.115, the "start time" protection mechanism can be bypassed because fork() is not atomic, and the

## Risk And Classification

**Problem Types:** CWE-362

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Polkit Project</a>	<a href="#">Polkit</a>	0.115	All	All	All
Application	<a href="#">Polkit Project</a>	<a href="#">Polkit</a>	0.115	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
[security-announce] openSUSE-SU-2019:1914-1: important: Security update	SUSE	<a href="#">lists.op</a>
[SECURITY] [DLA 1799-2] linux security update	MLIST	<a href="#">lists.de</a>
1692 - project-zero - Project Zero - Monorail	MISC	<a href="#">bugs.cf</a>
[SECURITY] [DLA 1799-1] linux security update	MLIST	<a href="#">lists.de</a>
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
USN-3903-2: Linux kernel (HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
USN-3908-2: Linux kernel (Trusty HWE) vulnerability   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
USN-3901-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
USN-3901-2: Linux kernel (HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
USN-3908-1: Linux kernel vulnerability   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
USN-3903-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
Red Hat Customer Portal	REDHAT	<a href="#">access</a>

backend: Compare PolkitUnixProcess uids for temporary authorizations (119) · Merge Requests · polkit / polkit · GitLab	MISC	<a href="#">gitlab.tr</a>
USN-3934-2: PolicyKit vulnerability   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
Merge branch 'uid-compare' into 'master' (c898fdf4) · Commits · polkit / polkit · GitLab	MISC	<a href="#">gitlab.fr</a>
USN-3934-1: PolicyKit vulnerability   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="#">git.kern</a>
PolicyKit CVE-2019-6133 Unauthorized Access Vulnerability	BID	<a href="#">www.se</a>
USN-3910-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
USN-3910-2: Linux kernel (Xenial HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubi</a>
[SECURITY] [DLA 1644-1] policykit-1 security update	MLIST	<a href="#">lists.de</a>
<a href="#">support.f5.com/csp/article/K22715344</a>	CONFIRM	<a href="#">support</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[377154](#) Alibaba Cloud Linux Security Update for polkit (ALINUX3-SA-2022:0004)

[377174](#) Alibaba Cloud Linux Security Update for polkit (ALINUX2-SA-2019:0013)

[378305](#) Virtuozzo Linux Security Update for polkit-docs (VZLSA-2019:0420)

© [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](#)