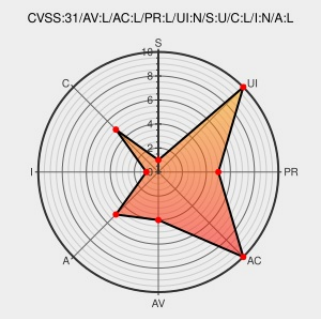
CVE-2019-15030

Published on: 09/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

CVE-2019-15030

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

In the Linux kernel through 5.2.14 on the powerpc platform, a local user can read vector registers of other users' processes via a Facility Unavailable exception. To exploit the venerability, a local user starts a transaction (via the hardware transactional memory instruction tbegin) and then accesses vector registers. At some point, the vector registers will be corrupted with the values from a different local Linux process because of a missing arch/powerpc/kernel/process.c check.

CVE-2019-15030 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	LOW

CVSS2 Score: 3.6 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
USN-4135-2: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory	UBUNTU USN-4135-2

USN-4135-2: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4135-2
USN-4135-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4135-1
September 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20191004-0001/
[security-announce] openSUSE-SU-2019:2181-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2019:2181
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2020:0740
[security-announce] openSUSE-SU-2019:2173-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2019:2173
oss-security - CVE-2019-15030: Linux kernel: powerpc: data leak with FP/VMX triggerable by unavailable exception in transaction	Mailing List Patch Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2019/09/10/3
kernel/git/torvalds/linux.git - Linux kernel source tree	Exploit Mailing List Patch Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8205d5d98ef7f155de211f5e2eb6ca03d95a5a60

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All

Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report