



CVE-2019-18660

Published on: 11/27/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:07 PM UTC

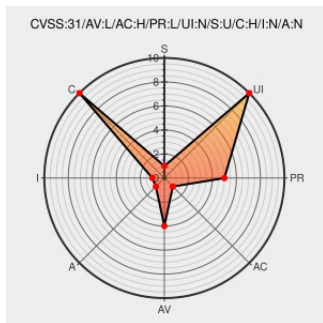
CVE-2019-18660

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The Linux kernel before 5.4.1 on powerpc allows Information Exposure because the Spectre-RSB mitigation is not in place for all applicable CPUs, aka CID-39e72bf96f58. This is related to arch/powerpc/kernel/entry_64.S and arch/powerpc/kernel/security.c.

CVE-2019-18660 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.7 - MEDIUM**

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

CVSS2 Score: **1.9 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2020:0174
Bugtraq: [slackware-security] Slackware 14.2	Mailing List	BUGTRAQ 20200109 [slackware-security] Slackware 14.2

kernel (SSA:2020-008-01)	Third Party Advisory seclists.org text/html	kernel (SSA:2020-008-01)
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	 MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=39e72bf96f5847ba87cc5bd7a3ce0fed813dc9ad
[SECURITY] Fedora 31 Update: kernel-5.3.14-300.fc31 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-b86a7bdba0
USN-4228-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4228-1
USN-4228-2: Linux kernel (Xenial HWE) vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4228-2
USN-4226-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4226-1
	Release Notes Vendor Advisory cdn.kernel.org text/plain	 CONFIRM cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.4.1
USN-4225-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4225-1
oss-security - CVE-2019-18660: Linux kernel: powerpc: missing Spectre-RSB mitigation	Mailing List Patch Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20191128 CVE-2019-18660: Linux kernel: powerpc: missing Spectre-RSB mitigation
USN-4227-2: Linux kernel (Azure) vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4227-2
December 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	Third Party Advisory security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20200103-0001/
[security-announce] openSUSE-SU-2019:2675-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2019:2675
USN-4227-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4227-1
Slackware Security Advisory - Slackware 14.2 kernel Updates ~ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/155890/Slackware-Security-Advisory-Slackware-14.2-kernel-Updates.html
USN-4225-2: Linux kernel (HWE) vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4225-2
[SECURITY] Fedora 30 Update: kernel-5.3.14-200.fc30 - package-announce - Fedora Mailing-	Third Party Advisory lists.fedoraproject.org	 FEDORA FEDORA-2019-124a241044

Lists

text/html

oss-security - CVE-2019-18660: Linux kernel: powerpc: missing Spectre-RSB mitigation

Mailing List

Patch

Third Party Advisory

www.openwall.com

text/html

MISC www.openwall.com/lists/oss-security/2019/11/27/1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	14.04	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	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	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	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	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	6.0	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:14.04:***:esm:***:						
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:19.10:****:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:esm:***:						
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:19.10:****:***:						
cpe:2.3:o:fedoraproject:fedora:30:****:***:						
cpe:2.3:o:fedoraproject:fedora:31:****:***:						
cpe:2.3:o:fedoraproject:fedora:30:****:***:						
cpe:2.3:o:fedoraproject:fedora:31:****:***:						
cpe:2.3:o:linux:linux_kernel:****:***:						
cpe:2.3:o:linux:linux_kernel:****:***:						
cpe:2.3:o:opensuse:leap:15.1:****:***:						
cpe:2.3:o:opensuse:leap:15.1:****:***:						

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:
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:6.0:*:*:*:*:*:
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 2023   |

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