



CVE-2019-13648

Published on: 07/19/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

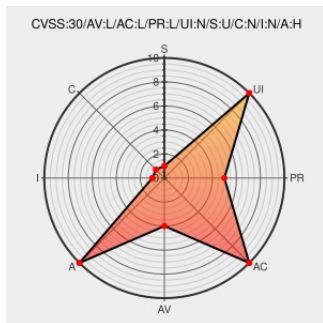
CVE-2019-13648

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

In the Linux kernel through 5.2.1 on the powerpc platform, when hardware transactional memory is disabled, a local user can cause a denial of service (TM Bad Thing exception and system crash) via a sigreturn() system call that sends a crafted signal frame. This affects arch/powerpc/kernel/signal_32.c and arch/powerpc/kernel/signal_64.c.

CVE-2019-13648 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **4.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4495-1 linux	www.debian.org Deprecated Link text/html	DEBIAN DSA-4495

July 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20190806-0001/
Debian -- Security Information -- DSA-4497-1 linux	www.debian.org Depreciated Link text/html	 DEBIAN DSA-4497
oss-security - CVE-2019-13648: Linux kernel: powerpc: kernel crash in TM handling triggerable by any local user	www.openwall.com text/html	 MLIST [oss-security] 20190730 CVE-2019-13648: Linux kernel: powerpc: kernel crash in TM handling triggerable by any local user
[security-announce] openSUSE-SU-2019:1924-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2019:1924
Slackware Security Advisory - Slackware 14.2 kernel Updates ~ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/154059/Slackware-Security-Advisory-Slackware-14.2-kernel-Updates.html
USN-4116-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4116-1
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	 CONFIRM git.kernel.org/torvalds/c/f16d80b75a096c52354c6e0a574993f3b0dfbdfc
USN-4114-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4114-1
Bugtraq: [SECURITY] [DSA 4495-1] linux security update	seclists.org text/html	 BUGTRAQ 20190812 [SECURITY] [DSA 4495-1] linux security update
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-226-01)	seclists.org text/html	 BUGTRAQ 20190814 [slackware-security] Slackware 14.2 kernel (SSA:2019-226-01)
[SECURITY] Fedora 30 Update: kernel-headers-5.2.5-200.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-7aecfe1c4b
USN-4115-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4115-1
powerpc/tm: Fix oops on sigreturn on systems without TM - Patchwork	Patch Third Party Advisory patchwork.ozlabs.org text/html	 MISC patchwork.ozlabs.org/patch/1133904/
Bugtraq: [SECURITY] [DSA 4497-1] linux security update	seclists.org text/html	 BUGTRAQ 20190813 [SECURITY] [DSA 4497-1] linux security update
[SECURITY] [DLA 1885-1] linux-4.9 security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20190814 [SECURITY] [DLA 1885-1] linux-4.9 security update
[security-announce] openSUSE-SU-2019:1923-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2019:1923

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	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:						

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](#)