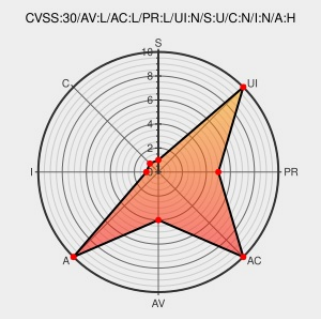
# CVE-2019-13648

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 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<br>Depreciated Link<br>text/html | DEBIAN DSA-4495 |

| | | |
|---|---|---|
| July 2019 Linux Kernel Vulnerabilities in NetApp Products \| NetApp Product Security | security.netapp.com<br>text/html | CONFIRM security.netapp.com/advisory/ntap-20190806-0001/ |
| Debian -- Security Information -- DSA-4497-1 linux | www.debian.org<br>Depreciated Link<br>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<br>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<br>text/html | SUSE openSUSE-SU-2019:1924 |
| Slackware Security Advisory - Slackware 14.2 kernel Updates ≈ Packet Storm | packetstormsecurity.com<br>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<br>text/html | UBUNTU USN-4116-1 |
| kernel/git/torvalds/linux.git - Linux kernel source tree | git.kernel.org<br>text/html | CONFIRM git.kernel.org/torvalds/c/f16d80b75a096c52354c6e0a574993f3b0dfbdfe |
| USN-4114-1: Linux kernel vulnerabilities \| Ubuntu security notices \| Ubuntu | usn.ubuntu.com<br>text/html | UBUNTU USN-4114-1 |
| Bugtraq: [SECURITY] [DSA 4495-1] linux security update | seclists.org<br>text/html | BUGTRAQ 20190812 [SECURITY] [DSA 4495-1] linux security update |
| Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-226-01) | seclists.org<br>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<br>text/html | FEDORA FEDORA-2019-7aecfe1c4b |
| USN-4115-1: Linux kernel vulnerabilities \| Ubuntu security notices \| Ubuntu | usn.ubuntu.com<br>text/html | UBUNTU USN-4115-1 |
| powerpc/tm: Fix oops on sigreturn on systems without TM - Patchwork | Patch<br>Third Party Advisory<br>patchwork.ozlabs.org<br>text/html | MISC patchwork.ozlabs.org/patch/1133904/ |
| Bugtraq: [SECURITY] [DSA 4497-1] linux security update | seclists.org<br>text/html | BUGTRAQ 20190813 [SECURITY] [DSA 4497-1] linux security update |
| [SECURITY] [DLA 1885-1] linux-4.9 security update | lists.debian.org<br>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<br>text/html | SUSE openSUSE-SU-2019:1923 |

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→