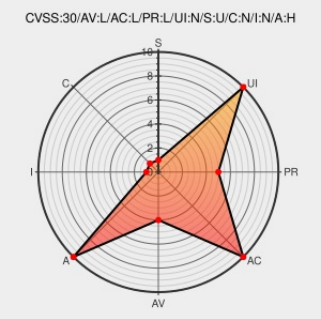
# CVE-2017-12192

Published on: 10/11/2017 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:28:00 PM UTC

## CVE-2017-12192

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




Certain versions of Linux Kernel from Linux contain the following vulnerability:

The keyctl_read_key function in security/keys/keyctl.c in the Key Management subcomponent in the Linux kernel before 4.13.5 does not properly consider that a key may be possessed but negatively instantiated, which allows local users to cause a denial of service (OOPS and system crash) via a crafted KEYCTL_READ operation.

CVE-2017-12192 has been assigned by secalert@redhat.com 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 |
|---|---|---|
| CVE-2017-12192 - Red Hat Customer Portal | access.redhat.com text/html | MISC access.redhat.com/security/cve/CVE-2017-12192 |
| | Vendor Advisory | CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.13.5 |

| | | |
|---|---|---|
| | Vendor Advisory<br>www.kernel.org<br>text/plain | CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.15.3 |
| Red Hat Customer Portal | access.redhat.com<br>text/html | REDHAT RHSA-2018:0151 |
| LKML: Eric Biggers: [PATCH] KEYS: prevent KEYCTL_READ on negative key | Mailing List<br>Third Party Advisory<br>lkml.org<br>text/xml | MISC lkml.org/lkml/2017/9/18/764 |
| Red Hat Customer Portal | access.redhat.com<br>text/html | MISC access.redhat.com/errata/RHSA-2018:0654 |
| KEYS: prevent KEYCTL_READ on negative key · torvalds/linux@37863c4 · GitHub | Patch<br>Vendor Advisory<br>github.com<br>text/html | CONFIRM github.com/torvalds/linux/commit/37863c43b2c6464f252862bf2e9768264e961678 |
| kernel/git/torvalds/linux.git - Linux kernel source tree | Patch<br>Vendor Advisory<br>git.kernel.org<br>text/html | CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=37863c43b2c6464f252862bf2e9768264e961678 |
| USN-3583-2: Linux kernel (Trusty HWE) vulnerabilities \| Ubuntu security notices | usn.ubuntu.com<br>text/html | UBUNTU USN-3583-2 |
| Red Hat Customer Portal | access.redhat.com<br>text/html | MISC access.redhat.com/errata/RHSA-2018:0181 |
| USN-3583-1: Linux kernel vulnerabilities \| Ubuntu security notices | usn.ubuntu.com<br>text/html | UBUNTU USN-3583-1 |
| Red Hat Customer Portal | access.redhat.com<br>text/html | MISC access.redhat.com/errata/RHSA-2020:2430 |
| oss-sec: CVE-2017-12192 kernel: NULL pointer dereference due to KEYCTL_READ on negative key | seclists.org<br>text/html | MISC seclists.org/oss-sec/2017/q4/63 |
| 1493435 – (CVE-2017-12192) CVE-2017-12192 kernel: NULL pointer dereference due to KEYCTL_READ on negative key | Issue Tracking<br>Third Party Advisory<br>bugzilla.redhat.com<br>text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1493435 |
| Red Hat Customer Portal | access.redhat.com<br>text/html | MISC access.redhat.com/errata/RHSA-2018:0152 |



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 |

System

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→