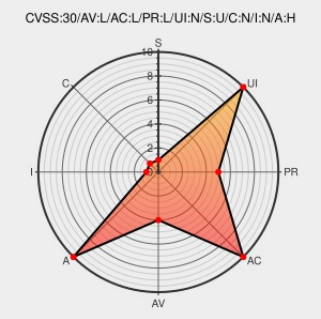
CVE-2017-15299

Published on: 10/14/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:32 PM UTC

CVE-2017-15299

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



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

The KEYS subsystem in the Linux kernel through 4.13.7 mishandles use of add_key for a key that already exists but is uninstantiated, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted system call.

CVE-2017-15299 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
[PATCH v3 1/7] KEYS: don't let add_key() update an uninstantiated key	Exploit, Issue Tracking, Mailing List	MISC www.mail-archive.com/linux-kernel@vger.kernel.org/msg1499828.html

	Patch Third Party Advisory www.mail-archive.com text/html	
USN-3798-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-3798-1
Bug 1498016 – CVE-2017-15299 kernel: Incorrect updates of uninstantiated keys crash the kernel	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1498016
USN-3798-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-3798-2
[SECURITY] [DLA 1200-1] linux security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20171210 [SECURITY] [DLA 1200-1] linux security update
'[PATCH v3 1/7] KEYS: don't let add_key() update an uninstantiated key' thread - MARC	Issue Tracking Patch Third Party Advisory marc.info text/html	MISC marc.info/?t=150654188100001&r=1&w=2
'[PATCH 12/15] KEYS: don't let add_key() update an uninstantiated key' thread - MARC	Issue Tracking Patch Third Party Advisory marc.info text/html	MISC marc.info/?t=150783958600011&r=1&w=2
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:0654

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→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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