CVE-2019-11487

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-11487
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-23 22:29:00 UTC
Updated	2023-02-24 18:43:00 UTC
Description	The Linux kernel before 5.1-rc5 allows page->_refcount reference count overflow, with resultant use-after-free issues, if abc

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.1	rc1	All	All
Operating System	Linux	Linux Kernel	5.1	rc2	All	All
Operating System	Linux	Linux Kernel	5.1	rc3	All	All
Operating System	Linux	Linux Kernel	5.1	rc4	All	All
Operating System	Linux	Linux Kernel	5.1	rc1	All	All
Operating System	Linux	Linux Kernel	5.1	rc2	All	All
Operating System	Linux	Linux Kernel	5.1	rc3	All	All
Operating System	Linux	Linux Kernel	5.1	rc4	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link

USN-4069-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com
Red Hat Customer Portal	REDHAT	access.redhat.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
USN-4069-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com
Merge branch 'page-refs' (page ref overflow) · torvalds/linux@6b3a707 · GitHub	MISC	github.com
[security-announce] openSUSE-SU-2019:1570-1: important: Security update	SUSE	lists.opensuse.org
Avoiding page reference-count overflows [LWN.net]	MISC	lwn.net
Red Hat Customer Portal	REDHAT	access.redhat.com
May 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
support.f5.com/csp/article/K14255532	CONFIRM	support.f5.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
USN-4118-1: Linux kernel (AWS) vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com
mm: make page ref count overflow check tighter and more explicit · torvalds/linux@f958d7b · GitHub	MISC	github.com
oss-security - Linux kernel: multiple issues	MLIST	www.openwall.com
Red Hat Customer Portal	REDHAT	access.redhat.com
mm: prevent get_user_pages() from overflowing page refcount · torvalds/linux@8fde12c · GitHub	MISC	github.com
mm: add 'try_get_page()' helper function · torvalds/linux@88b1a17 · GitHub	MISC	github.com
USN-4115-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com
fs: prevent page refcount overflow in pipe_buf_get · torvalds/linux@15fab63 · GitHub	MISC	github.com
[SECURITY] [DLA 1919-2] linux-4.9 security update	MLIST	lists.debian.org
[SECURITY] [DLA 1919-1] linux-4.9 security update	MLIST	lists.debian.org
[security-announce] openSUSE-SU-2019:1579-1: important: Security update	SUSE	lists.opensuse.org
[security-announce] openSUSE-SU-2019:1571-1: important: Security update	SUSE	lists.opensuse.org
1752 - project-zero - Project Zero - Monorail	MISC	bugs.chromium.org
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com
USN-4145-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Linux Kernel CVE-2019-11487 Multiple Denial of Service Vulnerabilities	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**