CVE-2016-5195

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-5195
State	PUBLIC
Assigner	chrome-cve-admin@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-11-10 21:59:00 UTC
Updated	2023-11-07 02:33:00 UTC
Description	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveragi

Risk And Classification

EPSS: 0.941760000 probability, percentile 0.999170000 (date 2026-04-02)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

Problem Types: CWE-362

CISA Known Exploited Vulnerability

Vendor	Linux
Product	Kernel
Name	Linux Kernel Race Condition Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2016-5195

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Core	15.04	All	All	All
Operating System	Canonical	Ubuntu Core	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All

Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	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	All	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Long Life	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Long Life	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Long Life	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Long Life	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Tus	6.5	All	All	All

References

Reference

[security-announce] SUSE-SU-2016:2632-1: important: Security update for

USN-3106-4: Linux kernel (Qualcomm Snapdragon) vulnerability | Ubuntu

PSIRT Advisories | FortiGuard

Bugtraq

USN-3104-1: Linux kernel vulnerability | Ubuntu

USN-3107-2: Linux kernel (Raspberry Pi 2) vulnerability | Ubuntu

[security-announce] SUSE-SU-2016:2596-1: important: Security update for

Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)

Debian -- Security Information -- DSA-3696-1 linux

DirtyCow Local Root Proof Of Concept ≈ Packet Storm

Red Hat Customer Portal

[SECURITY] Fedora 25 Update: kernel-4.8.3-300.fc25 - package-announce - Fedora Mailing-Lists

HPE Support document - HPE Support Center

[security-announce] SUSE-SU-2016:3069-1: important: Security update for

Red Hat Customer Portal - Access to 24x7 support and knowledge

Red Hat Customer Portal

[security-announce] SUSE-SU-2016:2659-1: important: Security update for

[security-announce] openSUSE-SU-2020:0554-1: important: Security update

Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW' Race Condition Privilege Escalation (SUID)

mm: remove gup_flags FOLL_WRITE games from __get_user_pages() · torvalds/linux@19be0ea · GitHub

oss-security - Re: CVE-2016-5195 test case

Bugtraq

kernel/git/torvalds/linux.git - Linux kernel source tree

Linux Kernel Dirty COW PTRACE_POKEDATA Privilege Escalation ≈ Packet Storm

oss-security - Re: CVE-2016-5195 "Dirty COW" Linux kernel privilege escalation vulnerability

[security-announce] SUSE-SU-2016:2631-1: important: Security update for

www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.8.3

oss-security - Re: CVE-2022-2590: Linux kernel: Modifying shmem/tmpfs files without write permissions

Red Hat Customer Portal

HPE Support document - HPE Support Center

PoCs · dirtycow/dirtycow.github.io Wiki · GitHub

[security-announce] SUSE-SU-2016:2629-1: important: Security update for

HPE Support document - HPE Support Center

Bugtraq

Android Security Bulletin—November 2016 | Android Open Source Project

Kernel Live Patch Security Notice LSN-0021-1 ≈ Packet Storm

CPU July 2018

Security Advisory - Dirty COW Vulnerability in Huawei Products

Red Hat Customer Portal

[security-announce] SUSE-SU-2016:2593-1: important: Security update for the Linux Kernel - openSUSE Security Announce - openSUSE Ma

USN-3105-1: Linux kernel vulnerability | Ubuntu

Linux Kernel CVE-2016-5195 Local Privilege Escalation Vulnerability

Red Hat Customer Portal

[SECURITY] Fedora 23 Update: kernel-4.7.9-100.fc23 - package-announce - Fedora Mailing-Lists

USN-3106-2: Linux kernel (Xenial HWE) vulnerability | Ubuntu

Cisco TelePresence Video Communication Server Test Validation Script Issue

[security-announce] SUSE-SU-2016:2637-1: important: Security update for Linux Kernel Live Patch 6 for SLE 12 SP1 - openSUSE Security A

[security-announce] SUSE-SU-2016:3304-1: important: Security update for

Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method)

HPE Support document - HPE Support Center

oss-security - CVE-2016-5195 "Dirty COW" Linux kernel privilege escalation vulnerability

[security-announce] SUSE-SU-2016:2585-1: important: Security update for

[security-announce] SUSE-SU-2016:2634-1: important: Security update for

Red Hat Customer Portal

Bugtraq

Vulnerability in Linux Kernel Affecting Cisco Products: October 2016

CVE-2016-5195 in Ubuntu

Vulnerability Note VU#243144 - Linux kernel memory subsystem copy on write mechanism contains a race condition vulnerability

Kernel Live Patch Security Notice LSN-0012-1 ≈ Packet Storm

Linux Kernel Dirty COW PTRACE_POKEDATA Privilege Escalation ≈ Packet Storm

[security-announce] SUSE-SU-2016:2673-1: important: Security update for

McAfee Security Bulletin: Fixes for privilege escalation via MAP_PRIVATE COW breakage (CVE-2016-5195)

HPE Support document - HPE Support Center

DirtyCow Linux Kernel Race Condition ≈ Packet Storm

CVE-2016-5195

oss-security - Re: CVE-2022-2590: Linux kernel: Modifying shmem/tmpfs files without write permissions

oss-security - Re: CVE-2022-2590: Linux kernel: Modifying shmem/tmpfs files without write permissions

CVE-2016-5195 - Red Hat Customer Portal

[security-announce] SUSE-SU-2016:2635-1: important: Security update for

McAfee Security Bulletin - Web Gateway update fixes the Huge Dirty Cow vulnerability (CVE-2017-1000405)

Bugtraq

HPE Support document - HPE Support Center

[security-announce] SUSE-SU-2016:2614-1: important: Security update for

Document Display | HPE Support Center

Bug 1004418 – VUL-0: CVE-2016-5195: kernel: local privilege escalation using MAP_PRIVATE "Dirty COW"

Knowledge Center

USN-3106-3: Linux kernel (Raspberry Pi 2) vulnerability | Ubuntu

[security-announce] SUSE-SU-2016:2657-1: important: Security update for

Bugtraq

Red Hat Customer Portal

Bug 1384344 – CVE-2016-5195 kernel: mm: privilege escalation via MAP_PRIVATE COW breakage

StruxureWare Data Center Operation Software Vulnerability Fixes - User Assistance for StruxureWare Data Center Operation 8 - Help Center

Red Hat Customer Portal

[security-announce] SUSE-SU-2016:2655-1: important: Security update for

[security-announce] openSUSE-SU-2016:2584-1: important: Security update for the Linux Kernel - openSUSE Security Announce - openSUS

oss-security - Re: CVE-2016-5195 "Dirty COW" Linux kernel privilege escalation vulnerability

USN-3105-2: Linux kernel (Trusty HWE) vulnerability | Ubuntu

Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method)

Security Advisory 0026 - Arista

USN-3106-1: Linux kernel vulnerability | Ubuntu

2017-01 Security Bulletin: Network and Security Manager (NSM): Multiple OpenSSH and other third party software vulnerabilities affect NSM A

Red Hat Customer Portal

2017-01 Security Bulletin: Junos Space: Multiple vulnerabilities resolved in 16.1R1 release. - Juniper Networks

Dirty COW (CVE-2016-5195)

[security-announce] SUSE-SU-2016:2636-1: important: Security update for Linux Kernel Live Patch 9 for SLE 12 - openSUSE Security Annou

Red Hat Customer Portal

[SECURITY] Fedora 23 Update: kernel-4.7.9-100.fc23 - package-announce - Fedora Mailing-Lists

[security-announce] SUSE-SU-2016:2638-1: important: Security update for Linux Kernel Live Patch 4 for SLE 12 SP1 - openSUSE Security A

Bugtraq

HPE Support document - HPE Support Center

[security-announce] SUSE-SU-2016:2592-1: important: Security update for

Red Hat Customer Portal

Bugtraq

[security-announce] SUSE-SU-2016:2658-1: important: Security update for

oss-security - Re: CVE-2022-2590: Linux kernel: Modifying shmem/tmpfs files without write permissions

oss-security - CVE-2016-5195 test case

CVE-2016-5195 Kernel Local Privilege Escalation Vulnerability in Multiple NetApp Products | NetApp Product Security

CVE-2016-5195 Kernel Local Privilege Escalation Vulnerability in Multiple NetApp Products | NetApp Product Security
[SECURITY] Fedora 24 Update: kernel-4.7.9-200.fc24 - package-announce - Fedora Mailing-Lists
Android Security Bulletin—December 2016 | Android Open Source Project
oss-security - CVE-2022-0847: Linux kernel: overwriting read-only files
[security-announce] SUSE-SU-2016:2630-1: important: Security update for
[SECURITY] Fedora 24 Update: kernel-4.7.9-200.fc24 - package-announce - Fedora Mailing-Lists
2017-10 Security Bulletin: Multiple Products: "Dirty COW" Linux Kernel Local Privilege Escalation (CVE-2016-5195) - Juniper Networks
oss-security - CVE-2022-2590: Linux kernel: Modifying shmem/tmpfs files without write permissions
Linux Kernel Copy-on-Write Memory Management Race Condition Lets Local Users Obtain Elevated Privileges - SecurityTracker
Red Hat Customer Portal
Kernel Local Privilege Escalation "Dirty COW" - CVE-2016-5195 - Red Hat Customer Portal
Broadcom Support Portal
[security-announce] SUSE-SU-2016:2633-1: important: Security update for
[SECURITY] Fedora 25 Update: kernel-4.8.3-300.fc25 - package-announce - Fedora Mailing-Lists
oss-security - Re: CVE-2022-2590: Linux kernel: Modifying shmem/tmpfs files without write permissions
VulnerabilityDetails · dirtycow/dirtycow.github.io Wiki · GitHub
[security-announce] openSUSE-SU-2016:2583-1: important: Security update
[security-announce] openSUSE-SU-2016:2625-1: important: Security update
USN-3104-2: Linux kernel (OMAP4) vulnerability | Ubuntu
USN-3107-1: Linux kernel vulnerability | Ubuntu
CVE-2016-5195 Kernel Vulnerability
Red Hat Customer Portal
[security-announce] openSUSE-SU-2016:2649-1: important: kernel update fo
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

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

site. This site includes MITRE data granted under the following license.

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