

CVE-2016-5195

Linux Kernel Race Condition Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

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 leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."

EVRS 79 / ₁₀₀ Urgent priority	CVSS V3.1 7.0 High · NVD	EPSS 0.835 99.69th percentile · FIRST	CISA DEADLINE Mar 24, 2022 KEV since 2022 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.835 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 10 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
cloud backup	—	no fixed version listed	NVD
hci storage nodes	—	no fixed version listed	NVD
oncommand balance	—	no fixed version listed	NVD
oncommand performance manager	—	no fixed version listed	NVD
oncommand unified manager for clustered data ontap	—	no fixed version listed	NVD
ontap select deploy administration utility	—	no fixed version listed	NVD
snapprotect	—	no fixed version listed	NVD
solidfire	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/torvalds/linux/commit/19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619

NVD nvd.nist.gov/vuln/detail/CVE-2016-5195

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2016-6146

Additional guidance access.redhat.com/errata/RHSA-2017:0372

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2016-5195

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.