Buffer overflow in drivers/xen/sys-hypervisor.c

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

Summary

CVE	CVE-2026-31786
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 11:16:20 UTC
Updated	2026-05-03 07:16:21 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: Buffer overflow in drivers/xen/sys-hypervisor.c The build ic

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000780000 probability, percentile 0.229230000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 e3af585e1728c917682b6a3de9a69b41fb9194d4 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 8288d031a01dbacfde3fc643f7be3d23504de64d git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 f458ba102da97fafca106327086fc95f3fc764cb git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 4b4defd2fce3f966c25adabf46644a85558f1169 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 5c5ff7c7bd15bb536f44b10b3fb5b8408f344d0a git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 d5f59216650c51e5e3fcb7517c825bc8047f60ef git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 52cecff98bda2c51eed1c6ce9d21c5d6268fb19d git
CNA	Linux	Linux	unaffected 5.10.254 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.204 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.170 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.137 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.85 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.26 6.18.* semver
CNA	Linux	Linux	unaffected 7.0.3 7.0.* semver

References

Reference	Source	Link	T
git.kernel.org/stable/c/5c5ff7c7bd15bb536f44b10b3fb5b8408f344d0a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/4b4defd2fce3f966c25adabf46644a85558f1169	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f458ba102da97fafca106327086fc95f3fc764cb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e3af585e1728c917682b6a3de9a69b41fb9194d4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/52cecff98bda2c51eed1c6ce9d21c5d6268fb19d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
www.openwall.com/lists/oss-security/2026/04/28/12	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
xenbits.xen.org/xsa/advisory-485.html	af854a3a-2127-422b-91ae-364da2661108	xenbits.xen.org	
git.kernel.org/stable/c/8288d031a01dbacfde3fc643f7be3d23504de64d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d5f59216650c51e5e3fcb7517c825bc8047f60ef	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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**