



KVM: nSVM: Always use vmcb01 in VMLOAD/VMSAVE emulation

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-43133
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:30 UTC
Updated	2026-05-08 17:25:23 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: KVM: nSVM: Always use vmcb01 in VMLOAD/VMSAVE e

Risk And Classification

Primary CVSS: v3.1 7.9 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000130000 probability, percentile 0.022800000 (date 2026-05-12)

Problem Types: NVD-CWE-noinfo

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.9	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:H
3.1	CNA	DECLARED	7.9	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

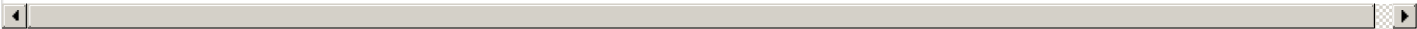
Integrity

Low

Availability

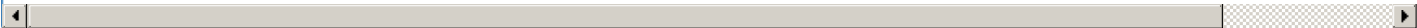
High

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



NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products			
Source	Vendor	Product	Version
CNA	Linux	Linux	affected cc3ed80ae69f454c3d904af9f65394a540099723 10063e1251c1485034a018236080792ad083dcc5 git
CNA	Linux	Linux	affected cc3ed80ae69f454c3d904af9f65394a540099723 c3b7015000988ba35ecd5648f4b2283960f00543 git
CNA	Linux	Linux	affected cc3ed80ae69f454c3d904af9f65394a540099723 3880e331b0b31d0d5d3702b124f6c93539cd478a git
CNA	Linux	Linux	affected cc3ed80ae69f454c3d904af9f65394a540099723 fce2fd4a2ca05670a91015aaccf96a1c26268fd git
CNA	Linux	Linux	affected cc3ed80ae69f454c3d904af9f65394a540099723 d464cf1ed900d47c85393d40b00017b6adfc2e6c git
CNA	Linux	Linux	affected cc3ed80ae69f454c3d904af9f65394a540099723 0004ecb798b30e90d7ebfe74efae2d9423315a64 git
CNA	Linux	Linux	affected cc3ed80ae69f454c3d904af9f65394a540099723 127ccae2c185f62e6ecb4bf24f9cb307e9b9c619 git
CNA	Linux	Linux	affected 5.13
CNA	Linux	Linux	unaffected 5.13 semver
CNA	Linux	Linux	unaffected 5.15.202 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix



References			
Reference	Source	Link	Tags
git.kernel.org/stable/c/127ccae2c185f62e6ecb4bf24f9cb307e9b9c619	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/10063e1251c1485034a018236080792ad083dcc5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/0004ecb798b30e90d7ebfe74efae2d9423315a64	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/d464cf1ed900d47c85393d40b00017b6adfc2e6c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c3b7015000988ba35ecd5648f4b2283960f00543	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch

git.kernel.org/stable/c/fce2fd4a2ca05670a91015aaccf96a1c26268fd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/3880e331b0b31d0d5d3702b124f6c93539cd478a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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