net/smc: fix NULL dereference and UAF in smc_tcp_syn_recv_sock()

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

Summary

CVE	CVE-2026-23450
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 16:16:31 UTC
Updated	2026-04-18 09:16:27 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix NULL dereference and UAF in smc_tcp_syn_

Risk And Classification

EPSS: 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected ebfee3e153f67c8b38eb94a7062ee94aa6f92708 f315277856caeafcd996c2611afc085ca2d53275 git
CNA	Linux	Linux	affected 8270d9c21041470f58348248b9d9dcf3bf79592e 1e4f873879e075bbd4eb1c644d6933303ac5eba4 git
CNA	Linux	Linux	affected 8270d9c21041470f58348248b9d9dcf3bf79592e f00fc26c8a06442b225a350fe000c0a11483e6a3 git
CNA	Linux	Linux	affected 8270d9c21041470f58348248b9d9dcf3bf79592e cadf3da46c15523fba90d80c9955f536ee3b4023 git
CNA	Linux	Linux	affected 8270d9c21041470f58348248b9d9dcf3bf79592e fd7579f0a2c84ba8a7d4f206201b50dc8ddf90c2 git
CNA	Linux	Linux	affected 8270d9c21041470f58348248b9d9dcf3bf79592e 1fab5ece76fb42a761178dcd0ebcbf578377b0dd git
CNA	Linux	Linux	affected 8270d9c21041470f58348248b9d9dcf3bf79592e 6d5e4538364b9ceb1ac2941a4deb86650afb3538 git
CNA	Linux	Linux	affected 5.18
CNA	Linux	Linux	unaffected 5.18 semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.20 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.10 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original commit for fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/cadf3da46c15523fba90d80c9955f536ee3b4023	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/fd7579f0a2c84ba8a7d4f206201b50dc8ddf90c2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1e4f873879e075bbd4eb1c644d6933303ac5eba4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f315277856caeafcd996c2611afc085ca2d53275	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/6d5e4538364b9ceb1ac2941a4deb86650afb3538	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f00fc26c8a06442b225a350fe000c0a11483e6a3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1fab5ece76fb42a761178dcd0ebcbf578377b0dd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
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.