



tipc: fix bc_ackers underflow on duplicate GRP_ACK_MSG

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

Summary

CVE	CVE-2026-31662
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:45 UTC
Updated	2026-04-24 17:51:40 UTC

Description In the Linux kernel, the following vulnerability has been resolved: tipc: fix bc_ackers underflow on duplicate GRP_ACK_MS

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 2f487712b89376fce267223bbb0db93d393d4b09 a7db57ccca21f5801609065473c89a38229ecb92 git
CNA	Linux	Linux	affected 2f487712b89376fce267223bbb0db93d393d4b09 36ec4fdd6250dcd5e73eb09ea92ed92e9cc28412 git
CNA	Linux	Linux	affected 2f487712b89376fce267223bbb0db93d393d4b09 575faea557f1a184a5f09661bd47ebd3ef3769f8 git
CNA	Linux	Linux	affected 2f487712b89376fce267223bbb0db93d393d4b09 3bcf7aca63f0bcd679ae28e9b99823c608e59ce3 git
CNA	Linux	Linux	affected 2f487712b89376fce267223bbb0db93d393d4b09 a2ea1ef0167d7a84730638d05c20ccdc421b14b6 git
CNA	Linux	Linux	affected 2f487712b89376fce267223bbb0db93d393d4b09 1b6f13f626665cac67ba5a012765427680518711 git
CNA	Linux	Linux	affected 2f487712b89376fce267223bbb0db93d393d4b09 e0bb732eaf77f9ac2f2638bdac9e39b81e0a9682 git
CNA	Linux	Linux	affected 2f487712b89376fce267223bbb0db93d393d4b09 48a5fe38772b6f039522469ee6131a67838221a8 git
CNA	Linux	Linux	affected 4.15
CNA	Linux	Linux	unaffected 4.15 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.169 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.135 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.82 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.23 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.13 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/48a5fe38772b6f039522469ee6131a67838221a8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3bcf7aca63f0bcd679ae28e9b99823c608e59ce3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a2ea1ef0167d7a84730638d05c20ccdc421b14b6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/575faea557f1a184a5f09661bd47ebd3ef3769f8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a7db57ccca21f5801609065473c89a38229ecb92	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/36ec4fdd6250dcd5e73eb09ea92ed92e9cc28412	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e0bb732eaf77f9ac2f2638bdac9e39b81e0a9682	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1b6f13f626665cac67ba5a012765427680518711	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

Free CVE JSON API cve.report/api

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