ksmbd: replace hardcoded hdr2_len with offsetof() in smb2_calc_max_out_buf_len()

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

Summary

CVE	CVE-2026-31478
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:16:44 UTC
Updated	2026-04-22 14:16:44 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: replace hardcoded hdr2_len with offsetof() in smb

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected f2283680a80571ca82d710bc6ecd8f8beac67d63 70b4c414889492c522b6e4331562360f49be2361 git
CNA	Linux	Linux	affected 9f297df20d93411c0b4ddad7f88ba04a7cd36e77 9a7166f0ef8cbb7bb48dd05e2471d995566003f5 git
CNA	Linux	Linux	affected e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d c3a89e3ec1ccf64fa6a34e391e1581ebbcba8683 git
CNA	Linux	Linux	affected e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d 6aef1765d6807e0f027cd87f6ac973eb0879a46d git
CNA	Linux	Linux	affected e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d 80824c7e527b70cf9039534e60aff592e8f209d1 git
CNA	Linux	Linux	affected e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d 4cb537ae4f37d7d0f617815ed4bed7173fb50861 git
CNA	Linux	Linux	affected e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d 0e55f63dd08f09651d39e1b709a91705a8a0ddcb gi
CNA	Linux	Linux	affected 6.6
CNA	Linux	Linux	unaffected 6.6 semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.131 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.80 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.21 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags

git.kernel.org/stable/c/6aef1765d6807e0f027cd87f6ac973eb0879a46d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0e55f63dd08f09651d39e1b709a91705a8a0ddcb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/80824c7e527b70cf9039534e60aff592e8f209d1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/4cb537ae4f37d7d0f617815ed4bed7173fb50861	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/70b4c414889492c522b6e4331562360f49be2361	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9a7166f0ef8cbb7bb48dd05e2471d995566003f5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c3a89e3ec1ccf64fa6a34e391e1581ebbcba8683	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.