

CVE-2026-98259

Microsoft fs/dax: check zero or empty entry before converting xarray entry

In the Linux kernel, the following vulnerability has been resolved: fs/dax: check zero or empty entry before converting xarray entry Calling dax_to_folio() with empty entry causes kernel panic below when booting a VM with DAX enabled storage. This patch checks empty entry before calling dax_to_folio() on dax_associate_entry(), dax_disassociate_entry(), and dax_busy_page().

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 5.5th percentile · FIRST	CISA DEADLINE — No CISA deadline
---	---------------------------------------	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

☐ CISA KEY	Not currently CISA KEY-listed	☐ Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
☐ Ransomware	Ransomware association unavailable	☐ KEV recency	CISA KEY listing date unavailable
☐ EPSS	0.002 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☐ CVSS	CVSS base score unavailable	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Monitor Untagged reference available; patch status is not confirmed

NVD lists one or more references for this CVE that aren't tagged as a patch or vendor advisory. Review them directly to confirm patch availability and applicability before making a remediation decision.

Basis: NVD reference (untagged)

Commit 98c183a4fccf ("fs/dax: don't disassociate zero page entries") added guards in the associate and disassociate paths, but the guards still come after dax_to_folio(), and dax_busy_page() still has the same problem. [0.737679] EXT4-fs (pmem0p1): mounted filesystem 79676804-7c8b-491a-b2a6-9bae3c72af70 ro with ordered data mode. Quota mode: disabled. [0.737891] VFS: Mounted root (ext4 filesystem) readonly on device 259:1. [0.739119] devtmpfs: mounted [0.739476] Freeing unused kernel memory: 1920K [0.740156] Run /sbin/init as init process [0.740229] with arguments: [0.740286] /sbin/init [0.740321] with environment: [0.740369] HOME=/ [0.740400] TERM=linux [0.743162] Unable to handle kernel paging request at virtual address fffffdffb0000008 [0.743285] Mem abort info: [0.743316] ESR = 0x0000000096000006 [0.743371] EC = 0x25: DABT (current EL), IL = 32 bits [0.743444] SET = 0, FnV = 0 [0.743489] EA = 0, S1PTW = 0 [0.743545] FSC = 0x06: level 2 translation fault [0.743610] Data abort info: [0.743656] ISV = 0, ISS = 0x00000006, ISS2 = 0x00000000 [0.743720] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [0.743785] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [0.743848] swapper pgtable: 4k pages, 48-bit VAs, pgdp=00000000b9d17000 [0.743931] [fffffdffb0000008] pgd=10000000bfa3d403, p4d=10000000bfa3d403, pud=1000000040bfe403, pmd=0000000000000000 [0.744070] Internal error: Oops: 0000000096000006 [#1] SMP [0.748888] CPU: 0 UID: 0 PID: 1 Comm: init Not tainted 6.18.4 #1 NONE [0.749421] pstate: 004000c5 (nzcw dalf +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [0.749969] pc : dax_disassociate_entry.constprop.0+0x20/0x50 [0.750444] lr : dax_insert_entry+0xcc/0x408 [0.750802] sp : ffff80008000b9e0 [0.751083] x29: ffff80008000b9e0 x28: 0000000000000000 x27: 0000000000000000 [0.751682] x26: 0000000001963d01 x25: ffff0000004f7d90 x24: 0000000000000000 [0.752264] x23: 0000000000000000 x22: ffff80008000bcc8 x21: 0000000000000001 [0.752836] x20: ffff80008000ba90 x19: 0000000001963d01 x18: 0000000000000000 [0.753407] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 [0.753970] x14: ffffbf3154b9ae70 x13: 0000000000000000 x12: ffffbf3154b9ae70 [0.754548] x11: ffffffff00000000 x10: 0000000000000000 x9: 0000000000000000 [0.755122] x8: 0000000000000000 x7: 0000000000000000 x6: 0000000000000000 [0.755707] x5: 0000000000000000 x4: 0000000000000000 x3: fffffdffc0000000 [0.756287] x2: 0000000000000000 x1: 0000000040000000 x0: fffffdffb0000000 [0.756871] Call trace: [0.757107]



dax_disassociate_entry.constprop.0+0x20/0x50 (P) [0.757592] dax_iomap_pte_fault+0x4fc/0x808 [0.757951]
dax_iomap_fault+0x28/0x30 [0.758258] ext4_dax_huge_fault+0x80/0x2dc [0.758594] ext4_dax_fault+0x10/0x3c
[0.758892] __do_fault+0x38/0x12c [0.759175] __handle_mm_fault+0x530/0xcfc [0.759518] handle_mm_fault+0xe4/0x230
[0.759833] do_page_fault+0x17c/0x4dc [0.760144] do_translation_fault+0x30/0x38 [0.760483] do_mem_abort+0x40/0x8c
[0.760771] el0_ia+0x4c/0x170 [0.761032] el0t_64_sync_handler+0xd8/0xdc [0.761371] el0t_64_sync+0x168/0x16c
[0.761677] Code: f9453021 f2dfbf3 cb813080 8b001860 (f9400401) [0.762168] ---[end trace 0000000000000000]---
[0.762550] note: init[1] exited with irqs disabled [0.762631] Kernel panic - not syncing: Attempted to kill init!
exitcode=0x0000000b

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
Not identified by the connected sources	–	no fixed version listed	NVD

Sources

Reference	git.kernel.org/stable/c/185cd2f5fe1e3319853cf065905b2885ad0bcbf8	Additional reference	git.kernel.org/stable/c/44ab7420ab52ab6c04bf225cac7c5c007cedd6c7
Additional reference	git.kernel.org/stable/c/8e2b8614039853e68d5338e37821e8bcee9fc05f	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98259
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93187	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98259

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.