

# CVE-2026-98469

## Microsoft KVM: arm64: Fix AArch32 DBG BXVR<n> handling

In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Fix AArch32 DBG BXVR<n> handling The consolidation of the breakpoint and watchpoint register accessors switched DBG BXVR<n> from trap\_bvr() to trap\_dbg\_wb\_reg(). The latter selects backing storage with demux\_wb\_reg(), which only handles Op2 values 4 through 7. Since DBG BXVR<n> uses Op2 1, an AArch32 guest access hits KVM\_BUG\_ON() and marks the VM dead.

| EVRS                   | CVSS       | EPSS                   | CISA DEADLINE    |
|------------------------|------------|------------------------|------------------|
| 0/100                  | —          | 0.002                  | —                |
| Informational priority | Not scored | 9th percentile · FIRST | No CISA deadline |

## Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

|                                     |                                    |                                                         |                                                                                                    |
|-------------------------------------|------------------------------------|---------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> CISA KEY   | Not currently CISA KEY-listed      | <input type="checkbox"/> Vendor exploitation            | Active-exploitation status not yet checked - scored at the population base rate (none) until known |
| <input type="checkbox"/> Ransomware | Ransomware association unavailable | <input type="checkbox"/> KEV recency                    | CISA KEY listing date unavailable                                                                  |
| <input type="checkbox"/> EPSS       | 0.002 probability                  | <input type="checkbox"/> Pre-patch disclosure           | Disclosure status unavailable                                                                      |
| <input type="checkbox"/> CVSS       | CVSS base score unavailable        | <input type="checkbox"/> 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)

DBG BXVR<n> aliases DBG BVR<n>\_EL1[63:32], and its AA32(HI) descriptor already selects the upper half. Map Op2 1 to dbg\_bvr[] alongside Op2 4, restoring the pre-regression behavior.

## Affected and fixed versions

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

## Sources

|                      |                                                                                                                                                         |                      |                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reference            | <a href="https://git.kernel.org/stable/c/6b1bca1b1ab77f60a62087337bfe6e2f0efb9e6d">git.kernel.org/stable/c/6b1bca1b1ab77f60a62087337bfe6e2f0efb9e6d</a> | Additional reference | <a href="https://git.kernel.org/stable/c/8530a05b304d312fe7dfbc5df7d3e87cc31b256a">git.kernel.org/stable/c/8530a05b304d312fe7dfbc5df7d3e87cc31b256a</a> |
| Additional reference | <a href="https://git.kernel.org/stable/c/af6813d16ace2765011ca1c567be86ade1d1ee8e">git.kernel.org/stable/c/af6813d16ace2765011ca1c567be86ade1d1ee8e</a> | NVD                  | <a href="https://nvd.nist.gov/vuln/detail/CVE-2026-98469">nvd.nist.gov/vuln/detail/CVE-2026-98469</a>                                                   |
| ENISA EUVD           | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-103709">euvd.enisa.europa.eu/vulnerability/EUVD-2026-103709</a>                           | Current data         | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2026-98469">evulnable.com/vulnerability-management/cve/CVE-2026-98469</a>               |

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