Broadcom patches critical vCenter authentication bypass (CVE-2026-123903) among 23 VMware fixes



Broadcom released patches for 23 VMware vulnerabilities, including CVE-2026-123903, a 9.8-rated authentication bypass in the vmdir directory service. The headline links it to earlier zero-day exploitation of vCenter.

- Broadcom patched 23 vulnerabilities across VMware ESX, vCenter, Workstation, Fusion and Avi Load Balancer.
- One flaw, CVE-2026-123903, is critical with a CVSS score of 9.8 out of 10.
- The bug sits in the VMware Directory Service (vmdir) and can allow authentication to be bypassed.
- The source headline describes it as following an earlier zero-day exploitation of vCenter.

Broadcom has released patches for 23 vulnerabilities affecting VMware ESX, vCenter, Workstation, Fusion and

Avi Load Balancer. One of them is rated critical.

What was reported

The critical flaw is tracked as **CVE-2026-123903** and scores 9.8 out of 10.0 on the CVSS scale. It resides in the VMware Directory Service, known as vmdir, and could be abused by a malicious actor to bypass authentication. The source headline presents this as a further critical vCenter flaw following a zero-day that was exploited earlier.

The excerpt available to us does not set out the full exploitation conditions, the affected version numbers or any workarounds. Those details should be taken from the Broadcom advisory itself.

Why it matters

vCenter is the management plane for virtualised estates, so an authentication bypass in a core component is a serious concern for any institution that relies on it. Given the earlier exploitation referenced in the headline, patching should not wait for a routine cycle.

Suggested next steps

Identify where vCenter and the other listed products run, read the Broadcom advisory for fixed versions, and schedule the update on a priority basis. Review management-interface exposure while you do so.

What to do now

1. Inventory all VMware vCenter, ESX and Avi Load Balancer instances and record their versions.
2. Read the Broadcom advisory for CVE-2026-123903 and apply the fixed versions on a priority, emergency-change basis.
3. Restrict vCenter management interfaces to dedicated administrative networks and confirm they are not internet-reachable.
4. Review vCenter and directory service logs for unexpected authentication events, given the earlier zero-day exploitation.
5. Record the patching decision and timeline in your vulnerability management and change records for audit.