Broadcom patches critical ESX and vCenter flaws among 23 VMware fixes



Broadcom released patches for 23 VMware vulnerabilities, including critical flaws in ESX and vCenter. The source reports no known exploitation in the wild, though Broadcom does not always flag it in advisories.

- The vCenter fixes cover seven bugs, including CVE-2026-123903, an authentication bypass in VMware Directory Service (CVSS 9.8).
- ESX updates fix seven issues, three of them critical and leading to code execution on the host: CVE-2026-123910, CVE-2026-123911 and CVE-2026-123912.
- Eight Avi Load Balancer flaws and one VMware Tools flaw were also patched.
- vCenter 8.0 U3m, released last week, already contains some fixes; vCenter 9.1.x, ESX, VMware Tools, Workstation, Fusion and Avi Load Balancer need updating.

> - Patches are cumulative, but SDDC Manager updates from VMSA-2026-0009 are not covered in this advisory.

Broadcom has released patches for 23 vulnerabilities across several VMware products, including critical-severity flaws in ESX and vCenter.

What was fixed

The vCenter updates resolve seven bugs. The most severe is **CVE-2026-123903**, an authentication bypass in VMware Directory Service with a CVSS score of 9.8. The same release addresses three denial-of-service issues in that service, a local privilege escalation in a vpxd service script, an arbitrary file write when processing certain archives, and a policy enforcement failure in the vSphere Distributed Switch.

The ESX updates also resolve seven issues. Three are critical and can lead to code execution on the host: CVE-2026-123910 and CVE-2026-123911 (CVSS 9.8) in the I/O filter service, and CVE-2026-123912 (CVSS 9.3) in the XHCI USB controller, which requires local administrative privileges on a virtual machine. Broadcom says that on ESX, exploitation is contained within the VMX sandbox.

Eight flaws in Avi Load Balancer, some allowing root-level code execution, and one denial-of-service flaw in VMware Tools were patched as well.

What needs updating

vCenter 8.0 U3m, released last week, already contains some of these fixes, so customers who applied it need not update again. vCenter 9.1.x, ESX, VMware Tools, Workstation, Fusion and Avi Load Balancer do need updates. Patches are cumulative and include fixes from VMSA-2026-0009, but this advisory does not cover the SDDC Manager updates from that earlier advisory, which must be handled separately.

Broadcom does not mention exploitation in the wild, although the source notes the company often does not warn of it in public advisories. Treat the absence of a warning as a reason to patch promptly, not to defer.

What to do now

1. Inventory all vCenter, ESX, VMware Tools, Workstation, Fusion and Avi Load Balancer instances and record their versions.
2. Confirm whether vCenter 8.0 U3m is already applied; prioritise vCenter 9.1.x and ESX hosts for patching.
3. Review Broadcom's advisory and schedule the updates through your change-management process, giving the critical CVEs priority.
4. Check that SDDC Manager updates from VMSA-2026-0009 have been handled, since this advisory does not cover them.
5. Restrict administrative access to vCenter and Avi Load Balancer management interfaces until patching is

complete.

6. Record patch status and any exceptions for reporting against your NCA ECC and SAMA CSF vulnerability-management controls.