Broadcom patches critical vCenter Server authentication bypass exploited since September 2026



Broadcom has released updates for a critical VMware vCenter Server authentication bypass flaw. Chinese-linked attackers reportedly exploited it as a zero-day from September 2026.

- The flaw is a critical authentication bypass in VMware vCenter Server.
- Broadcom has released security updates to fix it.
- It was exploited as a zero-day, according to the source since September 2026.
- The source attributes the attacks to Chinese-linked hackers.
- The source excerpt gives no CVE identifier or affected version details.

Broadcom, which now owns VMware, has released security updates for a critical authentication bypass

vulnerability in vCenter Server. According to BleepingComputer, hackers linked to China have been exploiting the flaw as a zero-day since September 2026, meaning attacks began before a fix was available.

Why it matters

vCenter Server is the central management point for virtualised environments. An authentication bypass on such a system can let an attacker act without valid credentials, so the exposure is significant for any organisation running it. The excerpt we reviewed does not name a CVE number, the affected versions or the technical details of the attacks, so those should be confirmed in Broadcom's own advisory.

What to do next

Institutions running vCenter Server should treat this as a priority patching item and verify the exact fixed versions against the vendor advisory. Because exploitation reportedly started months before the patch, applying the update may not be enough on its own; teams should also review whether there are signs of earlier compromise. Access to management interfaces should be limited to trusted administrative networks while the update is being scheduled.

What to do now

1. Identify all vCenter Server instances and confirm their versions against Broadcom's advisory.
2. Schedule emergency patching of affected instances using the released updates.
3. Restrict access to vCenter management interfaces to trusted administrative networks.
4. Review vCenter logs and administrator accounts for suspicious activity dating back to September 2026.
5. Report any confirmed compromise through your incident response process and to the relevant regulator as required.