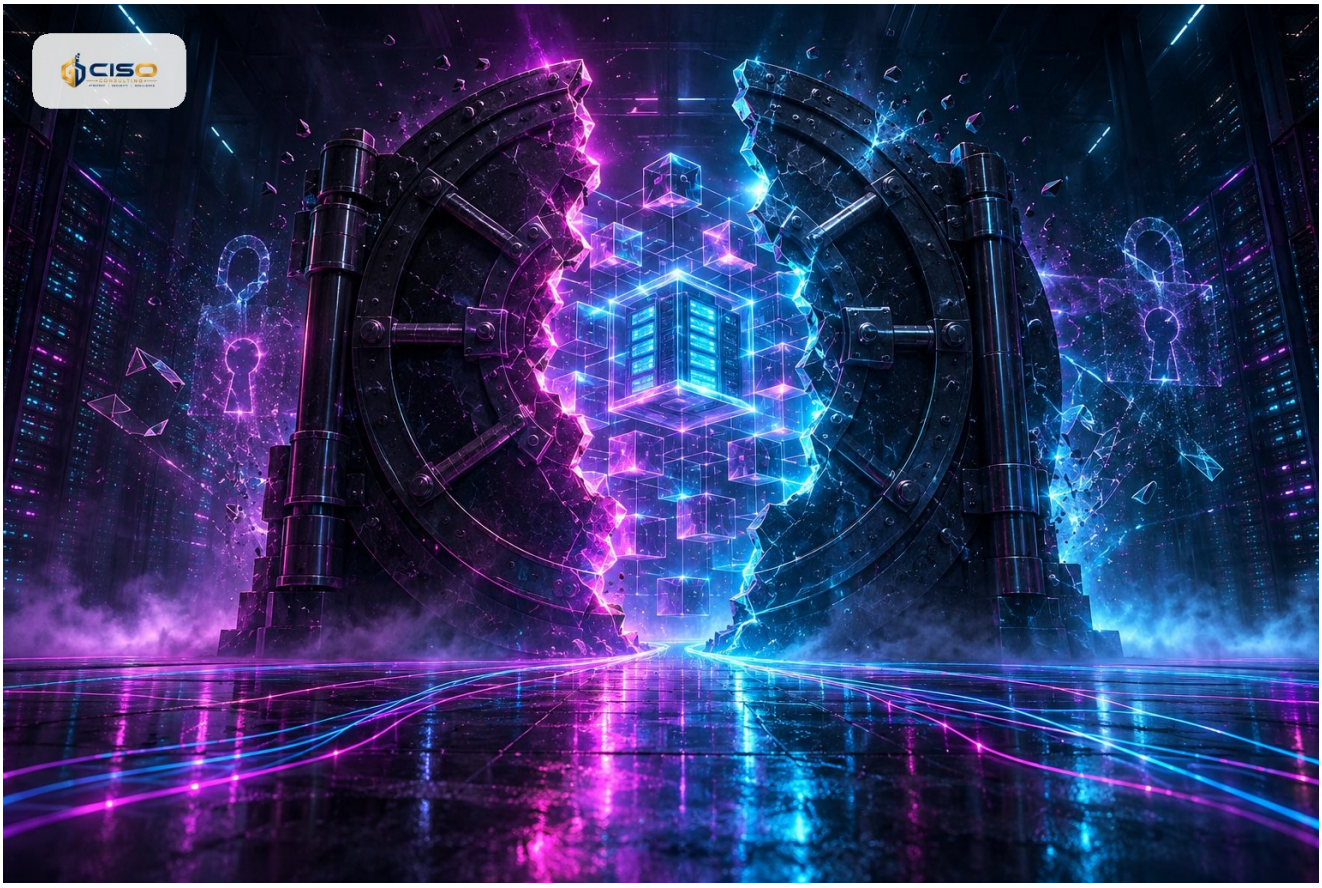
Critical VMware vCenter flaw (CVSS 9.8) allows authentication bypass over the network



Broadcom has published an advisory on a critical vCenter flaw that lets an attacker with network access bypass authentication. Fixed versions exist for all supported branches, and no workaround is listed.

- The flaw is rated CVSS 9.8 and affects VMware vCenter.
- An attacker with network access can bypass authentication and gain unauthorized access.
- Broadcom, which owns VMware, disclosed it in an advisory.
- Fixed versions are available for all supported branches.
- The vendor lists no workaround, so patching is the only remedy.

Broadcom, the owner of VMware, has published an advisory describing a critical vulnerability in VMware vCenter. The flaw is rated CVSS 9.8 and allows an attacker who can reach the system over the network to bypass authentication and obtain unauthorized access.

Why it matters

vCenter is the central console used to manage an organization's ESX hosts and virtual machines. Unauthorized access to it therefore touches the management layer of the virtualized environment, which is why institutions should treat the advisory as a priority.

What the vendor says

Fixed versions have been released for all supported branches. The company lists no workaround, so applying the update is the route to remediation. The source does not say whether the flaw is being exploited, and we make no claim about that.

Recommended approach

Teams should identify their vCenter instances, confirm the branch and version in use, and plan the update through the normal change process on an accelerated timeline. Until the update is applied, limiting who can reach the vCenter management interface on the network reduces exposure, though it does not replace the fix.

What to do now

1. Inventory all vCenter instances and record their versions and branches.
2. Check Broadcom's advisory for the fixed version that matches each branch.
3. Schedule the update on an accelerated emergency-change basis.
4. Restrict network access to vCenter management interfaces to authorized administrative networks until patched.
5. Review vCenter access and authentication logs for unexpected activity.