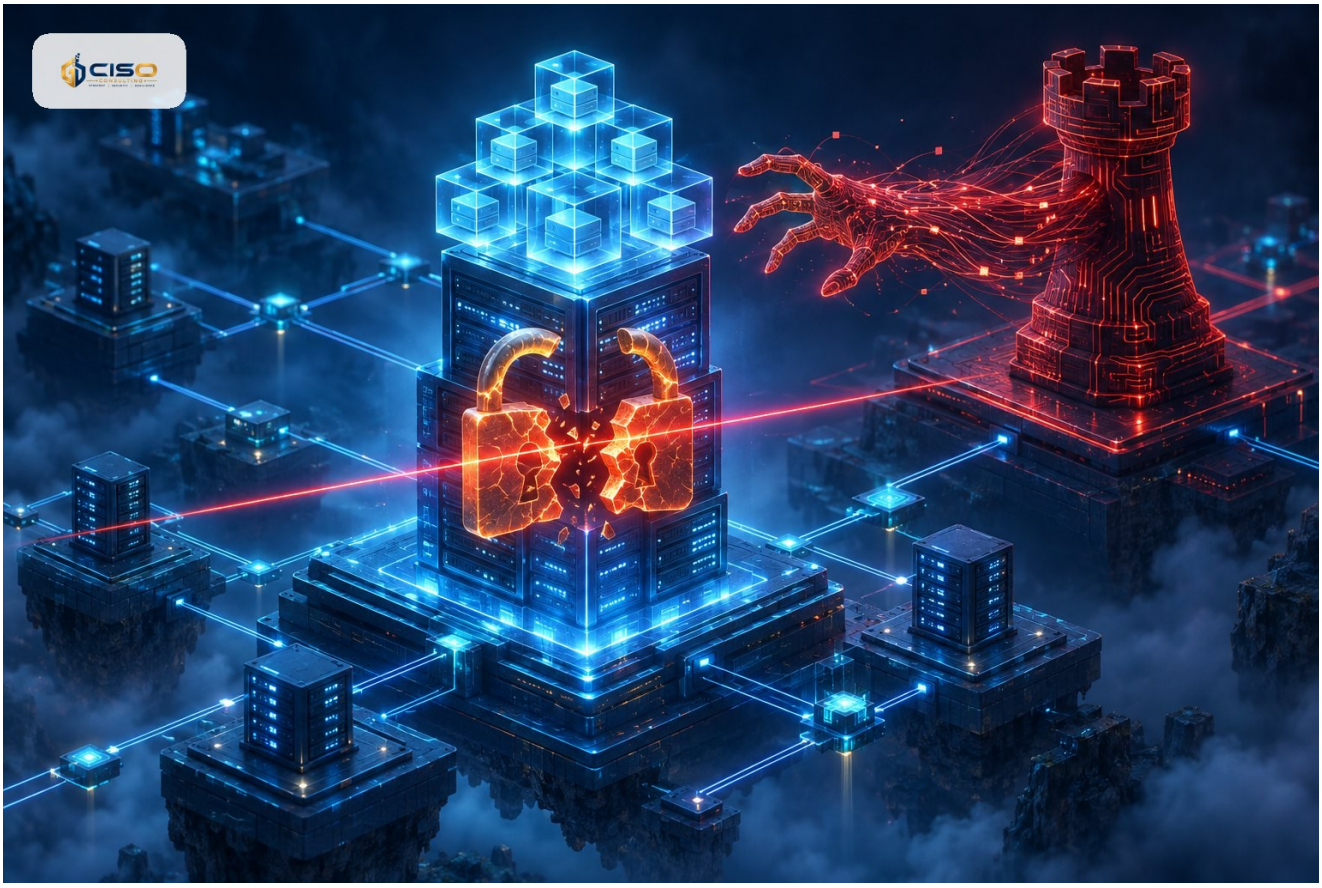
China-Linked Group Exploits Critical VMware vCenter Zero-Day (CVE-2026-123890)



A suspected China-nexus espionage group, Armory Castle (formerly UNC5221), reportedly exploited a critical VMware vCenter Server authentication bypass, CVE-2026-123890 (CVSS 9.8), as a zero-day in early September 2026.

- The group is tracked as Armory Castle, formerly UNC5221, and is suspected to be linked to China.
- The flaw is CVE-2026-123890, rated CVSS 9.8, in VMware vCenter Server.
- It is an authentication bypass in the VMware Directory Service.
- Exploitation as a zero-day was attributed to early September 2026.
- The report's headline says the attacks led to administrative access and data theft.

A suspected China-nexus cyber espionage group known as Armory Castle, formerly tracked as UNC5221, has been linked to zero-day exploitation of a critical flaw in VMware vCenter Server. According to the report, the activity took place in early September 2026.

What is known

The vulnerability is tracked as **CVE-2026-123890** and carries a CVSS score of 9.8. It is an authentication bypass in the VMware Directory Service. The report's headline states that exploitation gave attackers administrator access and allowed data theft. The excerpt available to us is truncated, so details on affected versions, patch availability, victims and technical indicators are not confirmed here.

Why it matters

vCenter Server manages virtualised infrastructure. An authentication bypass in a core service, exploited before a fix was available, means administrative control of a management plane can be obtained without valid credentials. Institutions that run VMware should treat this as a priority item and follow the vendor's guidance as it becomes available.

Suggested approach

Confirm whether vCenter is in use, limit who can reach it, and watch for unusual administrative activity. Check the vendor advisory for patch or workaround details before making changes, and document decisions for audit purposes.

What to do now

1. Identify all vCenter Server instances and record their versions.
2. Restrict network access to vCenter management interfaces to dedicated administrative networks.
3. Monitor the vendor's advisory and apply the patch or workaround once confirmed.
4. Review vCenter and directory service logs for unexpected administrator logins or account changes.
5. Rotate privileged credentials if suspicious activity is found, and escalate through your incident response process.