VMware vCenter zero-day CVE-2026-123890 exploited by China-linked group before patch



Broadcom has patched CVE-2026-123890, a critical vCenter flaw (CVSS 9.8) that a China-linked group exploited for over two months. vCenter 7.0 has no public patch, so affected organizations should patch and also check for compromise.

- CVE-2026-123890 (CVSS 9.8) is in the VMware Directory Service and lets a remote, unauthenticated attacker obtain an administrator-level authenticated session.
- Google says exploitation ran for more than two months before Broadcom's patch; Mandiant links it to Armory Castle (also known as Warp Panda, formerly UNC5221).
- Initial access came through a BeyondTrust Remote Support zero-day, CVE-2026-102764, followed by pivoting to Linux appliances and then vCenter.
- Fixes are in vCenter 9.1.1.0200, 9.0.2.0200 and 8.0 U3m; vCenter 7.0 reached end of general

support in October 2025 and has no public patch.

- Broadcom's advisory does not mention in-the-wild exploitation, so patching alone is not enough; compromise checks are advised.

Google reports that a suspected Chinese espionage group exploited a zero-day in VMware vCenter for more than two months before Broadcom released a patch on Thursday. The flaw, CVE-2026-123890, carries a CVSS score of 9.8 and sits in the VMware Directory Service. A remote attacker without credentials could use it to obtain an authenticated session with administrator privileges.

What Mandiant observed

Mandiant, which reported the bug to Broadcom, attributes the activity to Armory Castle, also known as Warp Panda and formerly tracked as UNC5221. According to its findings, the group first entered through CVE-2026-102764, a recently patched BeyondTrust Remote Support zero-day. It then moved to Linux appliances on the internal network and targeted vCenter in early September.

Using a custom tool called Bonesaw, the attackers stole the LMDB database, extracted SAML signing material and created a single sign-on administrator account. A second tool was used to forge SAML tokens, and backdoors were installed. They also took the vCenter master encryption key and database credentials, then moved to an ESXi host. Bonesaw was run against a vCenter server that had already been patched for CVE-2026-59309, a separate authentication bypass disclosed in July.

Patch availability

Broadcom has released fixes in vCenter 9.1.1.0200, 9.0.2.0200 and 8.0 U3m. Mandiant says Bonesaw works against vCenter 7.x and 8.x. Version 7.0 reached end of general support in October 2025 and has no public patch. Broadcom's advisory does not mention exploitation in the wild.

Mandiant's CTO, Charles Carmakal, advises organizations to apply the patches and also examine their systems for signs of compromise.

What to do now

1. Identify every vCenter instance and its version, and upgrade to 9.1.1.0200, 9.0.2.0200 or 8.0 U3m as applicable.
2. For vCenter 7.0, which has no public patch, plan migration to a supported version and restrict network access to it in the meantime.
3. Hunt for compromise even on patched servers: review for unexpected SSO administrator accounts, forged SAML activity, unknown backdoors and unusual ESXi access.
4. If compromise is suspected, treat SAML signing material, the vCenter master encryption key and database credentials as exposed and plan to rotate them.

5. Confirm that BeyondTrust Remote Support is patched for CVE-2026-102764 and review remote-access appliances and internal Linux appliances.
6. Report confirmed incidents through your established escalation path, including to the National Cybersecurity Authority and your sector regulator where required.