contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# Broadcom VMware vCenter exploited

**CVE-2026-123890 · on CISA's exploited list since 20 November 2026**

## Analysis Report

Anyone running VMware vCenter must patch immediately — the CISA deadline of 23 November 2026 has passed. Confirm which vCenter version is installed and compare it against the fixed versions in the …

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 25 November 2026 |
| FACTS AS OF | 25 November 2026 | VERSION | 1.0 |
| SEVERITY | **Critical: CVSS 3.1 9.8** | STATUS | On CISA's exploited list; due 23 November 2026 |

**NamiQ** © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/broadcom-vmware-vcenter-cve-2026-123890

## The bottom line

> *Anyone running VMware vCenter must patch immediately — the CISA deadline of 23 November 2026 has passed. Confirm which vCenter version is installed and compare it against the fixed versions in the vendor's advisory (VMSA-2026-0009).*

## At a glance

| Fact | Detail |
|---|---|
| Product | Broadcom VMware vCenter (CVE-2026-123890) |
| Severity | Critical: 9.8 (CVSS 3.1) |
| CISA | On its exploited list since 20 November 2026. Deadline for US federal agencies: 23 November 2026. |
| Chance of exploitation (EPSS) | 0.05, the estimated chance in the next 30 days, as at 25 November 2026 |
| Ransomware use | Not recorded by CISA. That is not the same as none. |
| Fixed in | vCenter 9.1.1.0200, 9.0.2.0200, 8.0 U3m; Cloud Foundation 5.2.5. The vendor's advisory lists vCenter 7.0 as affected too (contact Broadcom Support); the CVE record does not include 7.0. |
| Who looks first | Anyone running VMware vCenter (versions 9.1.x, 9.0.x, 8.0, or 5.x), Cloud Foundation, vSphere Foundation, Telco Cloud Platform, or Telco Cloud Infrastructure. The vendor's advisory also lists vCenter 7.0; the CVE record does not. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run VMware vCenter, Cloud Foundation, vSphere Foundation, or a Telco Cloud product? | Nothing to do for this CVE. | Check which version is installed (next question). |
| Is your vCenter version 9.0.x, 9.1.x, 8.0, 5.x, or is it on a Telco Cloud product? | CVE record lists no other vCenter versions; for 7.0, review VMSA-2026-0009 with Broadcom. | A patch applies — check whether vCenter is network-accessible (next question). |

| | | |
|---|---|---|
| Can anyone on your network, or from the internet, reach the vCenter management interface? | Patch at next scheduled maintenance; isolated vCenter reduces exposure. | Treat as urgent — patch before the next business day. |

## What it is

The flaw is in the VMware Directory Service, which vCenter uses to control who is allowed in. An attacker who can reach vCenter over a network — without any username or password — can bypass that check and gain access to the system.

## Why it matters

The flaw carries a CVSSv3 score of 9.8. CWE-288 means the attacker finds a path around the login check rather than breaking it — no credentials are required, only network access. The VMware Directory Service is central to vCenter's access control. Our reading is that bypassing it on a virtualisation management platform is unusually consequential: an attacker would likely gain the same standing as a legitimate administrator over the entire virtual estate that vCenter instance manages.

## What the vendor's advisory says

We read one page on support.broadcom.com. In short:

- The same advisory (VMSA-2026-0009) also covers CVE-2026-123891, an SQL-injection flaw in SDDC Manager rated 8.1 (Important), plus CVE-2026-123892, CVE-2026-123893, CVE-2026-123894; detail on those three is not in the sources here.
- The vendor's advisory states no workaround exists for CVE-2026-123890; patching is the only remediation.
- The advisory was first published 19 November 2026 and updated 20 November 2026.
- For VMware Cloud Foundation 5.x, the vendor notes an async patching guide (KB88287) is available alongside the fixed version 5.2.5.

## Things people will get wrong

- Only internet-facing vCenter instances are at risk The record and CISA description both say network access is sufficient. Any host on the same network as vCenter — not only internet-facing deployments — can attempt to exploit this.
- vCenter 7.0 is not affected because no patch version is listed in the CVE record The vendor's advisory lists vCenter 7.0 as affected at 9.8. It is the CVE record that omits 7.0 from its ranges, not the advisory. Contact Broadcom Support for the fix.
- Restricting network access to vCenter is an adequate temporary workaround The vendor's advisory states no workaround exists. Restricting access reduces exposure but does not close

the flaw; patching is the only remediation named.

## How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

## Step 1: Find the vCenter version you run

- Log in to the vCenter Server Management Interface (VAMI) or the vSphere Client and note the full version and build number shown in the About screen.
- Compare against the fixed versions: 9.1.1.0200, 9.0.2.0200, 8.0 U3m, or 5.2.5 for Cloud Foundation — as listed in the vendor's advisory (VMSA-2026-0009).
- If on vCenter 7.0, check whether you hold a Broadcom extended support contract before requesting the patch from Broadcom Support.

```
vpxd --version
rpm -qa VMware-vpxd
```

## Step 2: Restrict network access while you prepare the patch

- Confirm that the vCenter management interface is not reachable from the internet; block it at the network perimeter if it is.
- If immediate blocking is not possible, limit access to known administrator source IPs at the firewall until patching is complete.

## Step 3: Apply the patch from the vendor's advisory

- Download and apply the update listed in VMSA-2026-0009 for your version: 9.1.1.0200, 9.0.2.0200, 8.0 U3m, or 5.2.5; for Telco Cloud products, follow KB463116.
- After patching, verify the new version appears in the management interface and matches the expected fixed build before reopening access.

## Step 4: Check for signs of exploitation if vCenter was exposed before patching

- Review the vCenter SSO audit log for authentication events that succeeded without a matching normal login request in the period before patching.

- Look for new administrative accounts, role assignments, or configuration changes in vCenter that no known administrator initiated during the exposure window.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

## Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are writing about CVE-2026-123890, an authentication bypass in VMware vCenter's Directory Service (CVSS 9.8, Critical). CISA added it on 20 November 2026 with a remediation deadline of 23 November 2026, which has now passed. We need to establish: do we run any version of VMware vCenter, Cloud Foundation, vSphere Foundation, or a Telco Cloud product, and if so, which version? The fixed versions are vCenter 9.1.1.0200, 9.0.2.0200, 8.0 U3m, and Cloud Foundation 5.2.5; vCenter 7.0 requires contacting Broadcom Support under an extended support contract. Please confirm in writing the installed version and when the patch will be in place.*

## Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Authentication events in the SSO audit log that succeeded without a matching normal login request in the authentication flow, particularly during the exposure window.
- New administrative accounts or unexpected role assignments in vCenter created during the exposure window that no known administrator recognises.
- Unexpected configuration changes — to networking, permissions, or virtual machines — in vCenter during the period before patching was applied.

## The weakness behind it

The record classes this as CWE-288 (Authentication Bypass Using an Alternate Path or Channel).

## Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record

says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

**Steps an attacker would likely take with this flaw**

| The step, in plain words | Stage of an attack | Why we think so |
|---|---|---|
| Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page. | Initial Access: getting in | An unauthenticated attacker with network access can exploit the bypass directly. If vCenter is reachable from the internet, this would likely match exploitation of a public-facing application. |
| External Remote Services (T1133): Using a remote-access service such as a VPN or remote desktop to get into the network. | Initial Access: getting in | vCenter is a remote management service. The record says network access alone is sufficient to exploit it, which would likely fit the external-remote-services initial-access pattern. |
| Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use. | Initial Access: getting in | After bypassing authentication, the attacker gains a session the system treats as legitimate, so the access would likely appear as valid account activity in logs, masking the intrusion. |

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

## The sources, in their words

CISA's catalogue entry:

> *Broadcom VMware vCenter contains an authentication bypass using an alternate path or channel vulnerability in the VMware Directory Service that allows an unauthenticated attacker with network access to vCenter to bypass authentication and gain unauthorized access to the system.*

The CVE record, published by Vmware on 19 November 2026:

> *VMware vCenter contains an authentication bypass vulnerability in the VMware Directory Service. Affected versions: 9.1.x (fixed in 9.1.1.0200); 9.0.x (fixed in 9.0.2.0200); 8.0 (fixed in 8.0 U3m); 5.x (fixed in 5.2.5). Telco Cloud Platform 3.0, 4.x, 5.0.x, 5.1.x, 5.2 and Telco Cloud Infrastructure 3.0 are also affected (see KB463116).*

Versions of VMware vCenter the record lists as affected:

- 9.1.x up to, but not including, 9.1.1.0200
- 9.0.x up to, but not including, 9.0.2.0200

- 8.0 up to, but not including, 8.0 U3m
- 5.x up to, but not including, 5.2.5

The affected ranges end before 9.1.1.0200, 9.0.2.0200, 8.0 U3m, 5.2.5. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of VMware Telco Cloud Platform the record lists as affected:

- 3.0
- 4.x
- 5.0.x
- 5.1.x
- 5.2

Versions of VMware Telco Cloud Infrastructure the record lists as affected:

- 3.0

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

## Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-123890
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

## Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-123890
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

## What we do not know yet

- What specific path or channel in the VMware Directory Service is bypassed — the vendor's advisory does not describe the technical mechanism.
- Whether CVE-2026-123892, CVE-2026-123893, and CVE-2026-123894 (also in VMSA-2026-0009) affect vCenter or other components, and what their severity scores are.
- Whether the patch for vCenter 7.0 under a Broadcom extended support contract has been released or is still being prepared.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 25 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

## Appendix 1. Severity decoded

**CVE-2026-123890**: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

| Metric | Value | What it means here |
|---|---|---|
| Attack vector | Network | Reachable over a network, with no need to be on the same segment. |
| Attack complexity | Low | No special conditions beyond the flaw itself. |
| Privileges required | None | No account is needed. |
| User interaction | None | No one has to do anything. |
| Scope | Unchanged | Damage stays inside the vulnerable component. |
| Confidentiality | High | Total loss of confidentiality. |
| Integrity | High | Total loss of integrity. |
| Availability | High | Total loss of availability. |

## Appendix 2. Timeline

| Date | Event |
|---|---|
| 19 November 2026 | CVE record published by Vmware. |
| 20 November 2026 | CISA added it to its list of exploited vulnerabilities. |
| 23 November 2026 | CISA's deadline for US federal agencies. |

## Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

| Your situation | Priority | Timeframe |
|---|---|---|
| VMware vCenter unpatched and reachable from the internet | High | Overdue — CISA deadline was 23 November 2026 |
| VMware vCenter unpatched and reachable only from an internal network | High | Patch immediately; network access alone is sufficient to exploit |
| Running vCenter 7.0 — the vendor's advisory lists it as affected; the CVE record does not | Medium | Contact Broadcom Support this week to clarify fix availability |

| | | |
|---|---|---|
| Running SDDC Manager — the same advisory addresses CVE-2026-123891, an 8.1 SQL-injection flaw | Medium | Review VMSA-2026-0009 for SDDC Manager patches this week |
| vCenter patched to the stated fixed version and confirmed | None | None for this CVE |

## Appendix 4. Definition of done

- Every Broadcom VMware vCenter you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

## Sources


- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-123890: https://www.cve.org/CVERecord?id=CVE-2026-123890
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: support.broadcom.com/web/ecx/support-content-notification/-/external: https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/39495