TransilienceAI

CVE-2026-123890

Vulnerability Report · TLP:CLEAR

Broadcom · VMware vCenter

25 Nov 2026

Version 19 · 10 of 21 sources

Compiled by Transilience from public reporting. May be shared without restriction.

Table of Contents

BRIEF . . . 3
- Bottom line . . . 3
- For the board . . . 3
- Are you exposed? . . . 3
- What to do . . . 3

TIMELINE . . . 4

AFFECTED PRODUCTS AND VERSIONS . . . 4

FIXED IN . . . 4

EXPLOITATION . . . 4

WHO IS EXPLOITING IT . . . 5

MITIGATIONS AND DETECTION . . . 5

ATT&CK; TECHNIQUES . . . 5

INDICATORS . . . 5

NOT KNOWN YET . . . 6

SOURCES . . . 6

ABOUT THIS REPORT . . . 6

Brief

EXPLOITED IN THE WILD — LISTED IN CISA KEV

"ARMORY CASTLE exploited this vulnerability in early September 2026 using BONESAW, according to forensic evidence." [2]

Bottom line

An unauthenticated vCenter authentication-bypass (CVE-2026-123890) was exploited by a suspected China-nexus actor to steal LMDB, SAML keys, and persist; apply Broadcom's patches immediately and assume compromise for exposed vCenter servers. [2,3,7]

For the board

A critical vCenter authentication bypass was actively exploited to steal keys and create admin access; patch now and treat exposed vCenter servers as potentially compromised.

Are you exposed?

Affects	How to check
VMware vCenter Server (vmdir) — versions before Broadcom fixes (8.0, 9.0, 9.1 and 7.x presumed affected). [1,3,7]	Inspect vCenter version/build via vSphere Client or vCenter appliance UI; check for 8.0, 9.0, 9.1 or 7.0 presence.

What to do

1. **Apply Broadcom's vCenter security updates immediately (see vendor advisory).** [1,2]
   Patches remediate the authentication-bypass exploited in the wild and are the only vendor-provided fix.
2. **Assume compromise for any exposed vCenter and perform incident response and forensic review.** [2,3]
   ARMORY CASTLE exfiltrated LMDB and SAML keys and created SSO admin accounts during exploitation.
3. **Restrict network access to TCP/2012 and vCenter management interfaces until patched.** [2,7]
   The vulnerable vmdir DCE/RPC interface is reachable on TCP 2012 and is required for the bypass.
4. **Search logs for suspicious SSO admin creation, LMDB access, STS key access and unusual API calls.** [2,7]
   Exploitation results include database (data.mdb/LMDB) retrieval, STS signing key theft, forged admin sessions and account creation.

Timeline

Date	Kind	What happened
early September 2026	EXPLOITATION	ARMORY CASTLE exploited CVE-2026-123890 using BONESAW, exfiltrating LMDB and hijacking SAML. [2] *“ARMORY CASTLE exploited this vulnerability in early September 2026 using BONESAW, according to forensic evidence.”* [2]
2026-11-19 published	DISCLOSURE	Broadcom disclosed CVE-2026-123890 and published patches; advisory called an emergency change. [1] *“"In an FAQ published with the advisory, the company says the issue "qualifies under ITIL methodologies as an emergency change," and urges organizations to consult their security staff immediately on timing."”* [1]
2026-11-19 published	DISCLOSURE	Mandiant/GTIG published details linking exploitation to Armory Castle and BONESAW. [2] *“On Nov. 19, 2026, VMware disclosed CVE-2026-123890, which impacts VMware vCenter Server deployments.”* [2]
2026-11-23 published	ADVISORY	CISA added CVE-2026-123890 to its Known Exploited Vulnerabilities catalog. [4] *“The Google Threat Intelligence Group reported that ARMORY CASTLE, a suspected espionage group linked to China, exploited this flaw in September, before Broadcom released fixes on November 19.”* [4]
2026-11-24 published	DISCLOSURE	Rapid7 published a technical analysis and PoC reproducing root command execution against vCenter 8.0.2.00400. [7] *“We reproduced the bypass against vCenter Server Appliance 8.0.2.00400, build 23929136, running Photon OS 4.0, and leveraged the resulting administrator connection through to root command execution.”* [7]

Affected products and versions

- vCenter 8.0, 9.0, and 9.1 are present (older and 7.x presumed affected). [1]
  “The bug is present in vCenter 8.0, 9.0, and 9.1, and in the vCenter builds that ship inside VMware Cloud Foundation, vSphere Foundation, and the Telco Cloud Platform and Telco Cloud Infrastructure products.” [1]
- Bonesaw works against vCenter 7.x and 8.x per Mandiant. [3]
  “According to Mandiant, Bonesaw works against vCenter 7.x and 8.x.” [3]

Fixed in

- vCenter fixes: 9.1.1.0200, 9.0.2.0200, and 8.0 U3m (Broadcom published these). [3]
  “Broadcom has released fixes in vCenter versions 9.1.1.0200, 9.0.2.0200, and 8.0 U3m.” [3]

Exploitation

- ARMORY CASTLE exploited CVE-2026-123890 in early September 2026 using BONESAW. [2]
  “ARMORY CASTLE exploited this vulnerability in early September 2026 using BONESAW, according to forensic evidence.” [2]

- Rapid7 reproduced bypass and root command execution against vCenter 8.0.2.00400 (PoC). [7]
  “We reproduced the bypass against vCenter Server Appliance 8.0.2.00400, build 23929136, running Photon OS 4.0, and leveraged the resulting administrator connection through to root command execution.” [7]
- CISA added CVE-2026-123890 to KEV citing active exploitation. [4]
  “The Google Threat Intelligence Group reported that ARMORY CASTLE, a suspected espionage group linked to China, exploited this flaw in September, before Broadcom released fixes on November 19.” [4]

Who is exploiting it

- ARMORY CASTLE (suspected China-nexus espionage group). [2]
  “ARMORY CASTLE exploited this vulnerability in early September 2026 using BONESAW, according to forensic evidence.” [2]

Mitigations and detection

- Apply vendor patches from Broadcom immediately; no vendor workaround listed. [1]
  “Fixed versions are out for all supported branches, and the company lists no workaround.” [1]
- Restrict access to TCP/2012 and management ports until patched. [7]
  “The vulnerable interface is exposed through DCE/RPC on TCP port 2012.” [7]
- Examine systems for LMDB, STS key access, forged SSO assertions, and new SSO admin accounts. [7]
  “The attack recovered the directory database and its Security Token Service (STS) signing key, forged an administrator API session, and used appliance administration features to create an account and enable SSH.” [7]

ATT&CK techniques

ID	Technique	Mapped from
T1005	**Data from Local System** MAPPED BY NEWSROOM	*“The attack recovered the directory database and its Security Token Service (STS) signing key, forged an administrator API session, and used appliance administration features to create an account and enable SSH.”* [7]
T1078	**Valid Accounts** MAPPED BY NEWSROOM	*“Our attack workflow used a forged assertion to create a local appliance superAdmin account, enable SSH and Bash, and execute commands as root through sudo.”* [7]

Indicators

Kind	Indicator
DOMAIN	`vsphere[.]local` [2]
SHA256	`AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050` [2]
SHA1	`1f1476617a050b8e30388e0f58ed80d83f01aa02` [7]
SHA1	`af03ad96cb799381bf8e9a30a412b4371e24729d` [7]

SHA1	`537b2d5753f213304824551077bddd51ed6693ae` [7]
SHA1	`f56a33e23fad8b8d340c8ca0887aebe1fb793bab` [7]

Not known yet

- exact count of affected or compromised vCenter instances
- whether all listed affected versions are vulnerable in every deployment
- public availability of BONESAW source code
- full list of victims or sectors targeted

Sources

#	Outlet	Article	Copy
1	**The Hacker News** 19 Nov 2026	Critical VMware vCenter Flaw (CVSS 9.8) Lets Network Attackers Bypass Authentication	archived copy
2	**cR0w** 19 Nov 2026	ARMORY CASTLE Exploits vSphere | Google Cloud Blog	archived copy
3	**SecurityWeek** 19 Nov 2026	Newly Patched VMware vCenter Flaw Exploited as Zero-Day by Chinese APT	archived copy
4	**GBHackers** 23 Nov 2026	CISA Warns Hackers Are Actively Exploiting Cisco, VMware, SAP, and Apache Vulnerabilities	archived copy
5	**Help Net Security** 23 Nov 2026	Cisco Expressway vulnerability exploited to breach internal networks (CVE-2026-76466) - Help Net Security	archived copy
6	**The Hacker News** 23 Nov 2026	■ Weekly Recap: VMware 0-Day, Java4Shell, NGINX2Root, Ruby2Shell, and a Whole Lot of Shell Trouble	archived copy
7	**Rapid7 blog** 24 Nov 2026	Rapid7	archived copy
8	**The Hacker News** 24 Nov 2026	VMware vCenter Hit by Another Critical 9.8-Rated Auth Bypass Flaw After Zero-Day Exploitation	archived copy
9	**Security Affairs** 24 Nov 2026	VMware patches critical vCenter authentication bypass and ESX flaws	archived copy
10	**Rapid7 blog** 25 Nov 2026	Rapid7	archived copy

About this report

Compiled by Transilience Newsroom from 10 public sources. Every quotation is checked against the article it cites; 3 statements were left out because the source did not bear them out. The status is never stated more strongly than its

quote shows. ATT&CK techniques marked “mapped by Newsroom” are our reading of the quoted behaviour, not the source's claim. Version 19, written 25 November 2026, 12:50 UTC (cve-report-2026-09-25c). TLP:CLEAR — may be shared without restriction. The live report: https://threatnews.transilience.cloud/report/cve/cve-2026-123890