contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

A 2.7 on the KEV list

CVE-2026-41709 · VMware ESX · VMSA-2026-0006

Assessment & Action Plan

A logging gap in ESX, scored 2.7, was added to CISA's exploited list on 28 October. It lets an administrator act without being logged. What that means for your investigations, which builds fix it, and the critical flaws that shipped in the same advisory.

PREPARED BY	Hung Le, NamiQ	DATE	2 November 2026
FACTS AS OF	28 October 2026	VERSION	1.1
SEVERITY	**Low: CVSS 3.1 2.7; in CISA KEV**	STATUS	Fixed in ESXi 9.1.0.0-25370933, 9.0.2.0100-25595025, 8.0 U3j-25429389

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/vmware-esx-cve-2026-41709

Update, 2 November 2026: this note now ends with a section on checking your own servers and projects with lattice-scan, for IT admins, AI agent skills and CI/CD, and the analysis report is reissued with it. Everything else is as of 28 October 2026; check CISA's catalog for any change since.

A vulnerability score tells you how bad a flaw is on its own. It cannot tell you what the flaw is useful for. On 28 October CISA added CVE-2026-41709, a VMware ESX logging flaw scored 2.7 out of 10, to its list of vulnerabilities that are being exploited. A flaw that does nothing by itself and appears on that list tells you something about how attackers use it.

This note is for you if you run VMware ESX, or investigate incidents in an environment that does. Everything is as of 28 October 2026 and every claim links to its source at the end. One caution on sourcing: Broadcom's advisory page needs a browser to render, so our reading of the fixed builds comes from the CVE record and published coverage of the advisory. Confirm the builds in the advisory itself before you act.

The short version

- CVE-2026-41709 (CWE-778, insufficient logging) is a flaw in VMware ESX. A malicious administrator can perform certain operations without them being logged. CVSS 3.1 2.7: network, high privileges required, a low integrity impact.
- It was published in July in advisory VMSA-2026-0006 and added to CISA's Known Exploited Vulnerabilities catalog on 28 October, due 11 November. Ransomware use is not recorded.
- Fixed in ESXi 9.1.0.0-25370933, ESXi 9.0.2.0100-25595025 and ESXi80U3j-25429389, per the published coverage and the CVE record. Check the advisory for your exact build.
- The same advisory fixes more serious flaws: two critical vCenter flaws (CVE-2026-59309 and CVE-2026-59310, both 9.8) and a VM escape in the VMXNET3 adapter (CVE-2026-47876, 9.3). Patch to the build that covers all five.
- Broadcom said in July it had found no evidence any of the issues was exploited. CISA's listing is newer and does not say how the flaw is used.

What the flaw is

ESX records what administrators do: logins, configuration changes, commands. That record is what you reach for when something has gone wrong. This flaw means certain operations by an administrator are not recorded. It is not a way in. It needs an administrator already. Its value is what it does after the way in.

Why a 2.7 is on a list of exploited vulnerabilities

CISA's Known Exploited Vulnerabilities catalog is for vulnerabilities it has evidence are being exploited. A listing is CISA's statement that exploitation has been seen; it does not say who, how

widely or since when. A flaw can only be on the list if CISA has evidence it is being used. So the listing is evidence that somebody has used a bug that makes administrative actions invisible.

Our reading, and it is a reading and not something the sources state, is that the value of this flaw is in covering tracks. An attacker who has reached administrator access on a hypervisor, perhaps through one of the other flaws in the same advisory or through stolen credentials, can use a logging gap to do things you would later want to prove or disprove: what they accessed, what they changed. A defender investigating afterwards has a gap where the evidence should be.

That is why a score that measures damage on its own misleads here. The damage is to your ability to find out what happened.

The advisory it came with

VMSA-2026-0006 is not a low-severity advisory. It contains:

- CVE-2026-59309 and CVE-2026-59310 (vCenter, 9.8 each): an authentication bypass and a directory traversal leading to code execution, both with network access.
- CVE-2026-47876 (ESX, VMXNET3 adapter, 9.3): an out-of-bounds write that lets a virtual machine administrator execute code on the host, a VM escape.
- CVE-2026-41703 (7.6, information disclosure or denial of service).
- CVE-2026-41709 (2.7), the subject of this note.

Broadcom classed the updates as an emergency change requiring immediate action and listed no workarounds, according to published coverage. A researcher reported on 11 August a spike in scanning of vCenter that they considered consistent with attempts against CVE-2026-59309. That is the researcher's observation, not Broadcom's statement.

Who is exposed

- Anyone running ESX 9.1.x, 9.0.x or 8.0 builds before those named above, and the VMware Cloud Foundation, vSphere Foundation and Telco Cloud Platform versions that include them.
- The exposure to this flaw is specific to people who already have administrator access. That includes the people you know, and the credentials, scripts and tools that act as them.
- The larger exposure is the rest of the advisory. If you have not applied it, you have not closed the vCenter flaws either.

Things people will get wrong

- "It is a 2.7, so it can wait." It is on the exploited list, with a deadline.
- "Only admins can use it, so it is not our problem." Attackers who have become admins can use it. It is the second step.
- "The host logs show nothing unusual." That is exactly what the flaw can produce.

- "We can patch ESX and ignore vCenter." The advisory's most serious items are in vCenter and the VMXNET3 adapter.

How we would triage it

This is our judgement.

- Patch to the build that covers the whole advisory, within CISA's window. You are patching for the critical flaws; this one rides along.
- Change how you investigate. Do not rely on one host's own logs. Collect from the systems around it: vCenter, your identity provider, your network, your backup system.
- Reduce who can be an administrator, and how. The flaw only matters to an attacker who has become one.

Step 1: builds and exposure

```
# On an ESXi host
vmware -vl
esxcli system version get

# Who has administrator access
esxcli system permission list
```

Record the build number for every host and compare with the fixed builds in VMSA-2026-0006. Include hosts in recovery sites and lab clusters.

Step 2: send logs somewhere an administrator cannot edit

```
# Forward ESXi logs to a remote syslog collector
esxcli system syslog config set --loghost='tcp://LOGHOST:514'
esxcli system syslog reload
```

Use a collector that ESX administrators do not control, and keep the copy for as long as you keep other evidence. A log that an attacker can edit on the host is a log that a gap like this can empty. An off-host copy captures what is sent before the operation, and from other systems.

Step 3: patch

- Update to the fixed ESXi build for your version: ESXi 9.1.0.0-25370933 or later, ESXi 9.0.2.0100-25595025 or later, or ESXi80U3j-25429389 or later.
- Apply the advisory's other fixes for vCenter and the VMXNET3 flaw. Broadcom's table names different builds for them, so confirm which single build carries all five.

- Use vCenter lifecycle tooling where you have it, and plan evacuations.

Step 4: investigate without trusting the host

- Review vCenter events, identity provider logs and network flow records for the periods when administrators were active.
- Look for administrative access from addresses and times that do not fit, and for configuration changes that do not appear in any change record.
- Compare what the host's own log says with what the surrounding systems say. A mismatch is the finding.
- Lock down management: restrict who can reach ESX directly, and use lockdown mode so that hosts are managed through vCenter.

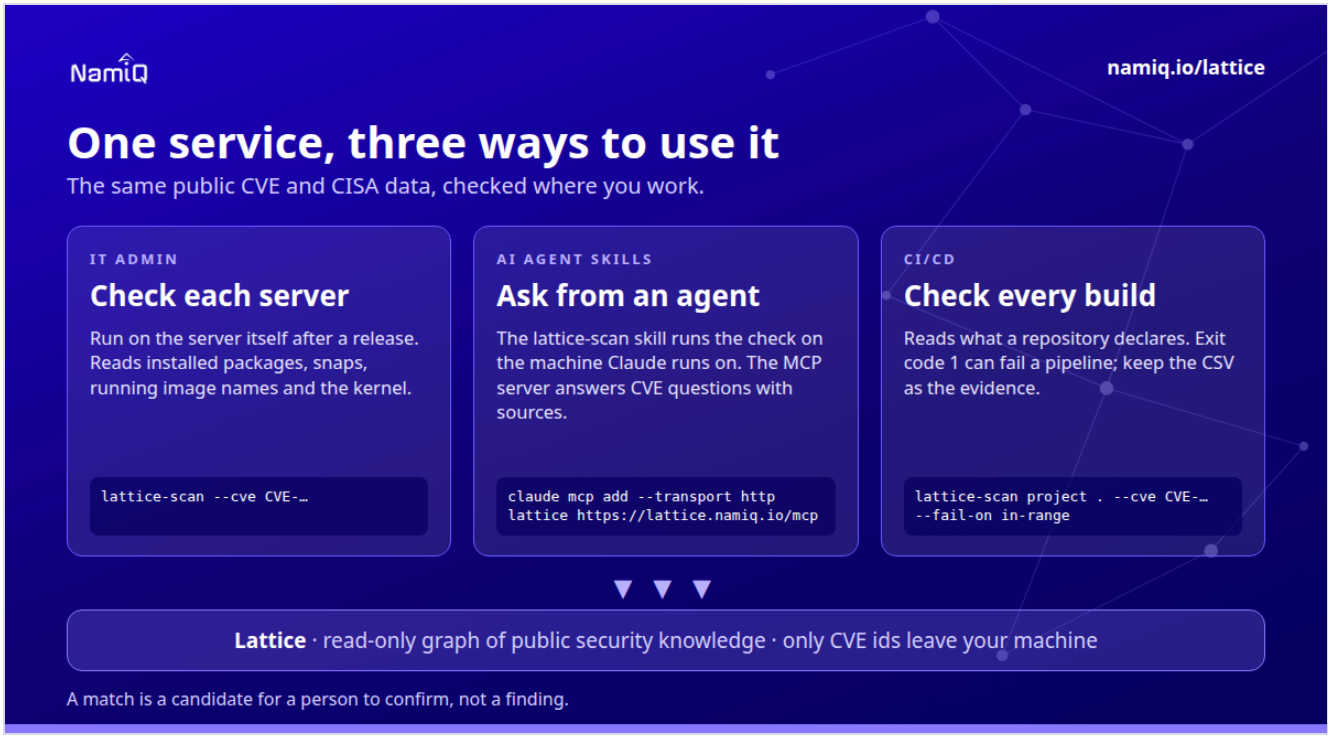
Check your own servers and projects

The facts above are as of 28 October 2026. lattice-scan, the open-source command line for checking this CVE against your own estate, cannot check this product: ESXi is not a Linux host with the package managers the host check reads, and a hypervisor is not declared in a project's manifests. Use VMware's own advisory tooling. A match from it would also never be a finding, only a candidate for a person to confirm.

What you can do instead: ask an AI agent connected to the Lattice MCP server to look up CVE-2026-41709. The keyless graph_lookup returns CISA's entry (listed, due date, required action) and the NVD entry (affected products and version ranges), each with its source. Then check the vendor's own advisory for your version. If you run Linux servers or build software around it, the command line still covers those parts.

Who can use it, and how

For	What to do	Command
AI agent skills	The lattice-scan skill runs the check on the machine Claude runs on. The Lattice MCP server answers questions about the CVE with its sources.	claude mcp add --transport http lattice https://lattice.namiq.io/mcp



Where the same check is used. The three ways read the same public data; only CVE ids leave your machine.

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

- How the flaw is being used. The listing gives no detail.
- Whether it is being used alone or with the vCenter and VMXNET3 flaws.
- Whether Broadcom's July statement about exploitation has changed.

If you take one thing from this: a good investigation does not depend on one witness. Make sure that a record of what an administrator did exists somewhere the administrator cannot reach.

Appendix 1. Severity decoded

CVE-2026-41709: score 2.7, `CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N` From the CVE record. High privileges required: the attacker is already an administrator.

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	High	An administrator account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	None	No data exposed.
Integrity	Low	Some data or behaviour can be altered.
Availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
29-30 July 2026	Broadcom publishes VMSA-2026-0006 and the CVE record. Broadcom says it has found no evidence any of the issues has been exploited in the wild.
11 August 2026	A researcher reports a spike in vCenter scanning consistent with possible attempts against CVE-2026-59309 (a researcher's observation, not Broadcom's).
28 October 2026	CISA adds CVE-2026-41709 to the Known Exploited Vulnerabilities catalog, due 11 November.

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
Any ESX host on an affected build, with administrator access held by more people or tools than you can list	High	Patch within the CISA window; log off-host now
ESX hosts whose logs are kept only on the host	High	Forward logs off-host this week

Hosts on a fixed build	None for this CVE	Confirm the build number
Environment without ESX	None	None

Appendix 4. Definition of done

- Every ESX host's exact build is known.
- Each is on a fixed build, and the same advisory's other fixes are in place.
- ESX logs are sent to a system that an ESX administrator cannot alter.
- Who holds administrator access to ESX, and how it is used, is known.
- Investigations do not rely on a single host's own logs as the only record of administrative activity.

Sources

- Broadcom advisory VMSA-2026-0006: https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017
- CVE-2026-41709 record (VMware CNA): https://www.cve.org/CVERecord?id=CVE-2026-41709
- The Hacker News: three critical VMware flaws allow authentication bypass (July 2026): https://thehackernews.com/2026/07/three-critical-vmware-flaws-allow-auth.html
- CISA Known Exploited Vulnerabilities catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog