

SECURITY ADVISORY

Canonical LXD: new CVE

CVE-2026-112816 · record published 30 October 2026

Analysis Report

If you run LXD or MicroCloud, update this week. The vendor calls the flaw critical and released fixes on 29 October 2026. First, check whether anything untrusted can reach the LXD HTTPS API. If you ...

PREPARED BY	NamiQ	DATE	31 October 2026
FACTS AS OF	31 October 2026	VERSION	1.0
SEVERITY	Critical: CVSS 4.0 10.0	STATUS	Not on CISA's exploited list; exploitation not recorded

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/canonical-lxd-cve-2026-112816

The bottom line

If you run LXD or MicroCloud, update this week. The vendor calls the flaw critical and released fixes on 29 October 2026. First, check whether anything untrusted can reach the LXD HTTPS API. If you run neither product, stop reading.

At a glance

Fact	Detail
Product	Canonical LXD (CVE-2026-112816)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by Canonical on 30 October 2026. Not on CISA's list of exploited vulnerabilities when we read it on 31 October 2026, which means nothing public says yet that anyone is using it.
Fixed in	lxd 6.10.1, 5.21.9, 5.0.11, 4.0.15; microcloud 2.1.5, 3.4.1 (snap, 29 October 2026)
Who looks first	Anyone running LXD or MicroCloud where the LXD HTTPS API can be reached by people or machines you do not fully trust. The advisory also names MicroCloud clusters where a new member is joining.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Canonical LXD or MicroCloud, on any host?	Nothing to do for this CVE.	Check the version (next question).
Is the version older than the fixed releases listed above for its channel?	You are on a fixed release. Confirm it in writing.	Go to the next question, then patch.
Is the LXD HTTPS API switched on for network access?	Exposure is lower, but still patch. The sources do not say this removes the risk.	Ask who can reach it (next question).
Can anyone outside your admin team reach that API port?	Patch in your normal cycle, but soon.	Restrict access now and patch first.

What it is

LXD's HTTPS API checked every certificate a client sent, but only the first one proves the client holds the key. The record says an attacker can put a trusted public certificate in the chain and be treated as that client, gaining full access to the cluster and its virtual machines.

Why it matters

The advisory says that, depending on the victim's privilege, the attacker may gain root access to the host. Our reading is that an LXD host is a good place for an attacker to stand: it controls the virtual machines on it. The attacker needs only a trusted client's public certificate, which is not a secret. The record gives this a score of 10 and the vendor calls it critical, so the fact that CISA does not yet list it should not lower your urgency.

What the vendor's advisory says

We read three pages on discourse.ubuntu.com. In short:

- The vendor's advisory says an attacker who can reach the LXD HTTPS API can authenticate as any trusted TLS client whose public certificate they hold.
- In MicroCloud, the advisory says an attacker can intercept the public certificate of a joining cluster member and then authenticate as that member.
- The advisory says all users must update to the latest version in their channel, using a snap refresh of lxd and of microcloud.
- The advisory says the point releases were still in progressive roll out from candidate to stable, so your host may not see the fix at once.
- The advisory says the issue was referred by the Incus project and confirmed to affect LXD as well.

Things people will get wrong

- "It is not on the CISA list, so it can wait." The record is new and CISA has not listed it. The vendor still calls it critical and urges updating immediately.
- "An attacker needs a login first." The record says the attacker is unauthenticated. The advisory says they need a trusted client's public certificate, which is not secret.
- "The snap refresh has already fixed us." The advisory says the releases were still rolling out to stable. Check the installed version against the fixed one.

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 versions you run

- List every host running LXD or MicroCloud, since the fix is per channel and each snap needs its own update.
- Compare each version with the fixed releases for its channel.

```
snap list lxd microcloud  
lxd --version  
snap info lxd
```

Step 2: Reduce exposure

- Find out whether the HTTPS API listens on the network and who can reach it.
- Limit that access to named administrator machines until the patch is in.

```
lxc config get core.https_address
```

Step 3: Patch

- The vendor's advisory says to run a snap refresh for lxd and for microcloud.
- If your channel has not received the fix yet, note it and check again, because the roll out was progressive.

Step 4: Check the result

- Confirm each host now reports a fixed version.
- Review client certificates the cluster trusts and remove any you do not recognise.

```
lxc config trust list
```

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.

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.

Hello, we need to know whether we run Canonical LXD or MicroCloud, and where. The vendor has published a critical flaw, CVE-2026-112816, in how the LXD HTTPS API checks client certificates. Please tell us which hosts run either product, which version each uses, and whether the HTTPS API can be reached from outside our admin network. The fixed versions are lxd 6.10.1, 5.21.9, 5.0.11 or 4.0.15, and microcloud 2.1.5 or 3.4.1. Please confirm in writing the installed versions and that the fix is applied, by the end of this week.

The weakness behind it

The record classes this as CWE-295.

The sources, in their words

The CVE record:

Improper certificate validation in the HTTPS listener in Canonical LXD 4.0.14, 5.0.10, 5.21.8, 6.9 before 4.0.15, 5.0.11, 5.21.9, 6.10.1 allows an unauthenticated attacker to authenticate as any trusted client and gain full access to the cluster and managed virtual machines via a crafted certificate chain.

Versions of Canonical LXD the record lists as affected:

- 4.0.14 up to, but not including, 4.0.15
- 5.0.10 up to, but not including, 5.0.11
- 5.21.8 up to, but not including, 5.21.9
- 6.9.0 up to, but not including, 6.10.1

What we do not know yet

- Whether the flaw is being used against real systems; CISA does not list it and the sources do not say.
- Whether turning off the network HTTPS API removes the risk; the sources do not say.
- Whether the fix has reached the stable channel for each release; the advisory says roll out was in progress.
- Whether the weakness leaves visible traces in logs; the sources do not say.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 31 October 2026. We read the vendor pages listed under Sources; nothing here has been

tested.

- 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", "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-2026-112816: score 10, CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H As the CVE record gives it.

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.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
30 October 2026	CVE record published by Canonical.

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
LXD API reachable from the internet or from untrusted networks	High	Today; restrict access, then patch

MicroCloud cluster, especially while a member is joining	High	Today; update microcloud and lxd
LXD API reachable only from a trusted management network	Medium	This week
LXD installed but the HTTPS API not enabled for the network	Low	Next patch cycle
No LXD or MicroCloud anywhere in your estate	None	None for this CVE

Appendix 4. Definition of done

- Every Canonical LXD you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-112816: <https://www.cve.org/CVERecord?id=CVE-2026-112816>
- CISA Known Exploited Vulnerabilities catalogue: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Advisory or release notes read: discourse.ubuntu.com/t/security-advisory-critical-vulnerability-found-in-canonical-lxd-and-microcloud/90557
- Advisory or release notes read: discourse.ubuntu.com/t/lxd-6-10-1-lts-has-been-released/90024: <https://discourse.ubuntu.com/t/lxd-6-10-1-lts-has-been-released/90024>
- Advisory or release notes read: discourse.ubuntu.com/t/lxd-5-21-9-lts-has-been-released/90565/1: <https://discourse.ubuntu.com/t/lxd-5-21-9-lts-has-been-released/90565/1>
- Reference in the CVE record: [github.com: https://github.com/canonical/lxd/security/advisories/GHSA-99jp-jwmc-65p4](https://github.com/canonical/lxd/security/advisories/GHSA-99jp-jwmc-65p4)
- Reference in the CVE record: [discourse.ubuntu.com: https://discourse.ubuntu.com/t/lxd-5-0-11-lts-has-been-released/90570/1](https://discourse.ubuntu.com/t/lxd-5-0-11-lts-has-been-released/90570/1)