Critical CVSS 10.0 flaw in LXD and MicroCloud allows client impersonation without a private key



A critical flaw in Canonical's LXD and MicroCloud lets an attacker authenticate as a trusted client using only its public certificate and network access to the HTTPS API, gaining access to the cluster and its virtual machines.

- The flaw affects Canonical's LXD and MicroCloud and is rated CVSS 10.0.
- An attacker can log in as a trusted client without holding that client's private key.
- Exploitation requires network reach to the HTTPS API and the trusted client's public certificate.
- A successful attacker acts as that client, with access to the cluster and its virtual machines.

What was reported

A critical vulnerability has been disclosed in Canonical's LXD and MicroCloud, scored CVSS 10.0, the maximum rating. It allows an attacker to authenticate as a trusted client without possessing that client's private key.

Conditions for exploitation

The attacker needs two things: network access to the HTTPS API of the affected deployment, and the public certificate of the trusted client to be impersonated. A public certificate is not normally treated as a secret, which is why the absence of any private-key requirement matters. Once authenticated, the attacker acts as that client and can reach the cluster and its virtual machines. The source text is truncated at the point where it discusses the impact if the impersonated account holds higher privileges, so the full consequences are not detailed here.

Why it matters

Institutions that use LXD or MicroCloud for private cloud or virtualization should treat this as a priority exposure, particularly where the API is reachable beyond a tightly controlled management network. The source does not provide patch versions, a CVE identifier or exploitation status, so teams should consult Canonical's official advisory for those details.

Until fixes are confirmed and applied, reducing who can reach the API is the most practical way to lower risk.

What to do now

1. Inventory all LXD and MicroCloud deployments, including clusters in test and development environments.
2. Restrict network access to the HTTPS API to dedicated management networks and approved hosts only.
3. Review Canonical's official advisory and apply the fixed versions as soon as they are confirmed.
4. Review API and cluster access logs for unexpected client activity and unfamiliar sources.
5. Review which trusted client certificates are registered and remove any that are unused or not needed.