Update of type field in restricted TLS certificate allows privilege escalation to cluster admin

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-34179
State	PUBLISHED
Assigner	canonical
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 10:16:21 UTC
Updated	2026-04-09 12:16:18 UTC
Description	In Canonical LXD versions 4.12 through 6.7, the doCertificateUpdate function in lxd/certificates.go does not validate the Typ

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from security@ubuntu.com

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

EPSS: 0.000870000 probability, percentile 0.251050000 (date 2026-04-10)

Problem Types: CWE-915 | CWE-915 CWE-915 Improperly controlled modification of Dynamically-Determined object attributes

Version	Source	Type	Score	Severity	Vector
3.1	security@ubuntu.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Canonical	Lxd	affected 4.12.0 5.0.7 semver	Linux
CNA	Canonical	Lxd	affected 5.1.0 5.21.5 semver	Linux
CNA	Canonical	Lxd	affected 6.0.0 6.8.0 semver	Linux

References

Reference	Source	Link	Tags
github.com/canonical/lxd/pull/17936	security@ubuntu.com	github.com	
github.com/canonical/lxd/security/advisories/GHSA-c3h3-89qf-jqm5	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: Miha Purg (en)

There are currently no legacy QID mappings associated with this CVE.