Exposed Session Token in canonical-livepatch client snap

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

Summary

CVE	CVE-2026-6369
State	PUBLISHED
Assigner	canonical
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-20 14:16:22 UTC
Updated	2026-04-20 19:05:30 UTC
Description	An improper access control vulnerability in the canonical-livepatch snap client prior to version 10.15.0 allows a local unprivil

Risk And Classification

Primary CVSS: v4.0 5.7 MEDIUM from security@ubuntu.com

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000170000 probability, percentile 0.042530000 (date 2026-04-22)

Problem Types: CWE-306 | CWE-732 | CWE-306 CWE-306 Missing authentication for critical function | CWE-732 CWE-732 Incorrect Permission Assignment for Critical Resource

Version	Source	Type	Score	Severity	Vector
4.0	security@ubuntu.com	Secondary	5.7	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:L/SA:L/E:X
4.0	CNA	CVSS	5.7	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:L/SA:L

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Canonical	Canonical-livepatch	affected 10.15.0 semver	Not specified

References

Reference	Source	Link	Tags
discourse.ubuntu.com/t/security-notice-canonical-livepatch-client-snap-vulnerabili...	security@ubuntu.com	discourse.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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