Leanote 2.7.0 - Local File Read

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

Summary

CVE	CVE-2024-0849
State	PUBLISHED
Assigner	Fluid Attacks
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-02-07 03:15:50 UTC
Updated	2026-04-20 16:16:38 UTC
Description	Leanote version 2.7.0 allows obtaining arbitrary local files. This is possible because the application is vulnerable to LFR.

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000280000 probability, percentile 0.079880000 (date 2026-04-21)

Problem Types: CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	help@fluidattacks.com	Secondary	5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Leanote	Desktop	2.7.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Leanote	Leanote	affected 2.7.0	Not specified

References

Reference	Source	Link	Tags
fluidattacks.com/advisories/alesso	af854a3a-2127-422b-91ae-364da2661108	fluidattacks.com	Third Party Advisory
github.com/leanote/desktop-app	af854a3a-2127-422b-91ae-364da2661108	github.com	Product
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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