



# Improper Restriction of Operations within the Bounds of a Memory Buffer in linkingvision rapidvms

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-33849
<b>State</b>	PUBLISHED
<b>Assigner</b>	GovTech CSG
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-24 06:16:22 UTC
<b>Updated</b>	2026-04-20 20:20:21 UTC
<b>Description</b>	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in linkingvision rapidvms.This issue a

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from cve\_disclosure@tech.gov.sg

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

**EPSS:** 0.000420000 probability, percentile 0.127440000 (date 2026-04-20)

**Problem Types:** CWE-119 | CWE-119 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Version	Source	Type	Score	Severity	Vector
3.1	cve_disclosure@tech.gov.sg	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linkingvision	Rapidvms	-	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Linkingvision	Rapidvms	affected PR#96 git	Not specified

### References

Reference	Source	Link	Tags
github.com/linkingvision/rapidvms/pull/96	cve_disclosure@tech.gov.sg	github.com	Issue Tracking
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** TITAN Team (titancaproject@gmail.com) (en)

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)