

CVE-2026-6499

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2026-6499
State	PUBLISHED
Assigner	TCS-CERT
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 14:16:36 UTC
Updated	2026-05-05 20:14:04 UTC
Description	Incorrect Permission Assignment for Critical Resource vulnerability in ILM Informatique OpenConcerto allows Replace Bina

Risk And Classification

Primary CVSS: v4.0 2.4 LOW from 64c5ae8f-7972-4697-86a0-7ada793ac795

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

EPSS: 0.000130000 probability, percentile 0.021580000 (date 2026-05-05)

Problem Types: CWE-732 | CWE-732 CWE-732: Incorrect Permission Assignment for Critical Resource

Version	Source	Type	Score	Severity	Vector
4.0	64c5ae8f-7972-4697-86a0-7ada793ac795	Secondary	2.4	LOW	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	2.4	LOW	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v4.0 Breakdown	
Attack Vector	Local
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User Interaction	Passive
Confidentiality	

None

ntegrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/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	ILM Informatique	OpenConcerto	affected 1.7.5	Not specified

References

Reference	Source	Link	Tags
www.openconcerto.org/fr/version-1.7.html	64c5ae8f-7972-4697-86a0-7ada793ac795	www.openconcerto.org	
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: Dominique Righetto (en)

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