



GeoVision GV-VMS V20 WebCam Server stack overflow vulnerability

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

Summary

CVE	CVE-2026-42369
State	PUBLISHED
Assigner	GV
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 01:16:04 UTC
Updated	2026-05-04 01:16:04 UTC
Description	GV-VMS V20 is a Video Monitoring Software used to gather the feeds of many surveillance cameras and manage other sec

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from 0df08a0e-a200-4957-9bb0-084f562506f9

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

Problem Types: CWE-787 | CWE-787 CWE-787 Out-of-bounds write

Version	Source	Type	Score	Severity	Vector
3.1	0df08a0e-a200-4957-9bb0-084f562506f9	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GeoVision Inc.	GV-VMS V20.0.2	affected V20.0.2	Windows
CNA	GeoVision Inc.	GV-VMS V20.0.2	unaffected V21.0.0	Windows

References

Reference	Source	Link	Tags
https://talosintelligence.com/vulnerability_reports	0df08a0e-a200-4957-9bb0-084f562506f9	https	
www.geovision.com.tw/cyber_security.php	0df08a0e-a200-4957-9bb0-084f562506f9	www.geovision.com.tw	
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: Philippe Laulheret of Cisco Talos. (en)

CNA: Kelly Patterson of Cisco Talos. (en)

CNA: Martin Zeiser of Cisco Talos. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-02-17T01:32:00.000Z	Initial Vendor Contact

Solutions

CNA: GeoVision GV-VMS version V21.0.0 has patched the reported vulnerability. User is recommended to download the update from GeoVision's official website (<https://www.geovision.com.tw/download/product/GV-VMS%20V20>) or contact GeoVision Support team

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

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

CVE.report and Source URL Uptime Status status.cve.report