GeoVision GV-VMS V20 WebCam Server Login stack overflow vulnerability

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

Summary

CVE	CVE-2026-42370
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	A stack overflow vulnerability exists in the WebCam Server Login functionality of GeoVision GV-VMS V20 20.0.2. A special

Risk And Classification

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

CVSS:3.1/AV:N/AC:H/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	9	CRITICAL	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9	CRITICAL	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/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 20.0.2	Windows
CNA	GeoVision Inc.	GV-VMS V20.0.2	unaffected 21.0.0	Windows

References

Reference	Source	Link	Tags
talosintelligence.com/vulnerability_reports	0df08a0e-a200-4957-9bb0-084f562506f9	talosintelligence.com	
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	2026-02-17T01:38:00.000Z	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 offical 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.

Free CVE JSON API cve.report/api

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