



GV-ASWeb Remote Code Execution (RCE) vulnerability

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

Summary

CVE	CVE-2026-7841
State	PUBLISHED
Assigner	GV
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 08:16:04 UTC
Updated	2026-05-06 08:16:04 UTC
Description	A remote code execution vulnerability exists in Notification Settings on GeoVision GV-ASWeb 6.2.0. An authenticated user

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from 0df08a0e-a200-4957-9bb0-084f562506f9

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

Problem Types: CWE-94 | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	0df08a0e-a200-4957-9bb0-084f562506f9	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GeoVision Inc.	ASManager	affected V6.2.0	Windows
CNA	GeoVision Inc.	ASManager	unaffected V6.3.0	Windows

References

Reference	Source	Link	Tags
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: Patrick Tung <patricktkc.work@gmail.com> (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-28T17:05:00.000Z	Initial report to vendor

Solutions

CNA: Reported Vulnerability is going to be fixed with the official release of GeoVision's ASManager V6.3.0

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

