



GeoVision LPC2011/LPC2211 Web Interface / ssi.cgi reflected cross-site scripting (XSS) vulnerabilities

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

Summary

CVE	CVE-2026-42366
State	PUBLISHED
Assigner	GV
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 01:16:03 UTC
Updated	2026-05-04 01:16:03 UTC
Description	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the Web Interface / ssi.cgi functionality of GeoVision LPC2

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from 0df08a0e-a200-4957-9bb0-084f562506f9

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

Problem Types: CWE-79 | CWE-79 CWE-79 Improper neutralization of input during web page generation ('cross-site scripting')

Version	Source	Type	Score	Severity	Vector
3.1	0df08a0e-a200-4957-9bb0-084f562506f9	Secondary	7.4	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	7.4	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GeoVision Inc.	GV-LPC2011/LPC2211	affected V1.10	Linux
CNA	GeoVision Inc.	GV-LPC2011/LPC2211	unaffected V1.20	Linux

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	2026-02-17T01:03:00.000Z	Initial Vendor Contact

Solutions

CNA: GeoVision GV-LPC2011/LPC2211 V1.12-260330 has patched the reported vulnerability. The user may visit GeoVision website or contact GeoVision Support team for firmware update.

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