



# GeoVision LPC2011/LPC2211 Web Interface / DdnsSetting.cgi OS command injection vulnerability

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

## Summary

<b>CVE</b>	CVE-2026-42364
<b>State</b>	PUBLISHED
<b>Assigner</b>	GV
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-04 01:16:03 UTC
<b>Updated</b>	2026-05-04 01:16:03 UTC
<b>Description</b>	An os command injection vulnerability exists in the DdnsSetting.cgi functionality of GeoVision LPC2011/LPC2211 1.10. A s

## Risk And Classification

**Primary CVSS:** v3.1 9.9 CRITICAL from 0df08a0e-a200-4957-9bb0-084f562506f9

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

**Problem Types:** CWE-78 | CWE-78 CWE-78 Improper neutralization of special elements used in an OS command ('OS command injection')

Version	Source	Type	Score	Severity	Vector
3.1	0df08a0e-a200-4957-9bb0-084f562506f9	Secondary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Changed**

Confidentiality

**High**

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GeoVision Inc.	GV-LPC2011/LPC2211	affected 1.10	Linux
CNA	GeoVision Inc.	GV-LPC2011/LPC2211	unaffected 1.12	Linux

### References

Reference	Source	Link	Tags
talosintelligence.com/vulnerability_reports	0df08a0e-a200-4957-9bb0-084f562506f9	<a href="https://talosintelligence.com">talosintelligence.com</a>	
www.geovision.com.tw/cyber_security.php	0df08a0e-a200-4957-9bb0-084f562506f9	<a href="https://www.geovision.com.tw">www.geovision.com.tw</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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	2026-02-17T00:00:00.000Z	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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)