

CVE-2024-11120

GeoVision Devices OS Command Injection Vulnerability

CISA KEV since May 7, 2025

Actively exploited

Certain EOL GeoVision devices have an OS Command Injection vulnerability. Unauthenticated remote attackers can exploit this vulnerability to inject and execute arbitrary system commands on the device. Moreover, this vulnerability has already been exploited by attackers, and we have received related reports.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.284 98.1st percentile · FIRST	CISA DEADLINE May 28, 2025 KEV since 2025 · listed over a year
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.284 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
gv-vs12 firmware	–	no fixed version listed	NVD
gv-vs11 firmware	–	no fixed version listed	NVD
gv-dsp lpr firmware	–	no fixed version listed	NVD
gvlx 4 firmware	–	no fixed version listed	NVD
gv-vs12	–	no fixed version listed	NVD
gv-vs11	–	no fixed version listed	NVD
gv-dsp lpr	3.0	no fixed version listed	NVD
gvlx 4	2.0 3.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-hq2j-jpv4-q865

dlcdn.geovision.com.tw dlcdn.geovision.com.tw/TechNotice/CyberSecurity/Security_Advisory_IP_Device_2024-11.pdf
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2024-11120

NVD nvd.nist.gov/vuln/detail/CVE-2024-11120

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-33664

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.