Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Hackers Exploit Zero-Day Flaw in EOL GeoVision Devices

Date of Publication	Admiralty Code	TA Number
November 18, 2024	A1	TA2024434

Summary

First Seen: November 14, 2024
Affected Product: GeoVision Devices
Malware: Mirai
Impact: CVE-2024-11120 is a critical OS command injection vulnerability in outdated GeoVision devices, allowing unauthenticated attackers to execute arbitrary commands remotely. Actively exploited in the wild, it has been used by botnets, such as Mirai, for DDoS and cryptomining. With no patches available, users are advised to isolate or replace the devices urgently.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-11120	GeoVision OS Command Injection Vulnerability	GeoVision Devices	✓	✗	✗

Vulnerability Details

#1 CVE-2024-11120 is a critical vulnerability (CVSS 9.8) identified in several end-of-life (EOL) GeoVision devices. It is an OS command injection flaw that allows unauthenticated remote attackers to execute arbitrary system commands. The vulnerability has been actively exploited by attackers, primarily through a botnet using a variant of the Mirai malware, often employed for DDoS attacks or cryptomining.

#2 The affected devices include GeoVision models such as GV-VS12, GV-VS11, GV-DSP LPR V3, and certain versions of GV-LX4C. Since these devices are EOL, no patches or updates are available to mitigate the flaw. Reports suggest around 17,000 vulnerable devices are exposed online, with most located in the United States, Germany, and Canada.

#3 It is recommended to disconnect these devices from the internet and replace them with supported alternatives. If replacement is not immediately feasible, they should be isolated within secure networks and closely monitored.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-11120	GeoVision VS12 GeoVision VS11 GeoVision DSP_LPR_V3 GeoVision LX 4 V2 GeoVision LX 4 V3	cpe:2.3:o:geovision:gvlx_4_v3_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gvlx_4_v2_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs12_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs11_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-dsp_lpr_v3_firmware:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Immediate Isolation: The first step is to remove affected EOL GeoVision devices from the network. Alternatively, place them behind a properly configured firewall to prevent remote access. This action helps to minimize exposure to potential attacks.

Device Replacement: Consider replacing these EOL devices with supported and up-to-date alternatives as soon as possible. Since these devices are no longer receiving patches or support from the manufacturer, replacement is crucial for long-term security.

Network Segmentation: If it is not feasible to remove the devices immediately, implement strict network segmentation. This approach limits their exposure and potential impact on other systems within the network.

Enhanced Monitoring: Implement enhanced monitoring for any suspicious activities or commands executed on these devices. Continuous monitoring can help in detecting unauthorized access attempts or exploitation attempts early.

Access Control: Strengthen access controls and authentication mechanisms for any networks where these devices are present. Ensure that only authorized personnel have access to these devices and their management interfaces.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0042 Resource Development	TA0002 Execution	T1498 Network Denial of Service
T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities	T1588 Obtain Capabilities	T1588.005 Exploits

Patch Details

No patch is available for CVE-2024-11120, as it affects end-of-life GeoVision devices with no vendor support; users must replace or isolate the devices to mitigate the risk.

References

https://www.twcert.org.tw/en/cp-139-8237-26d7a-2.html

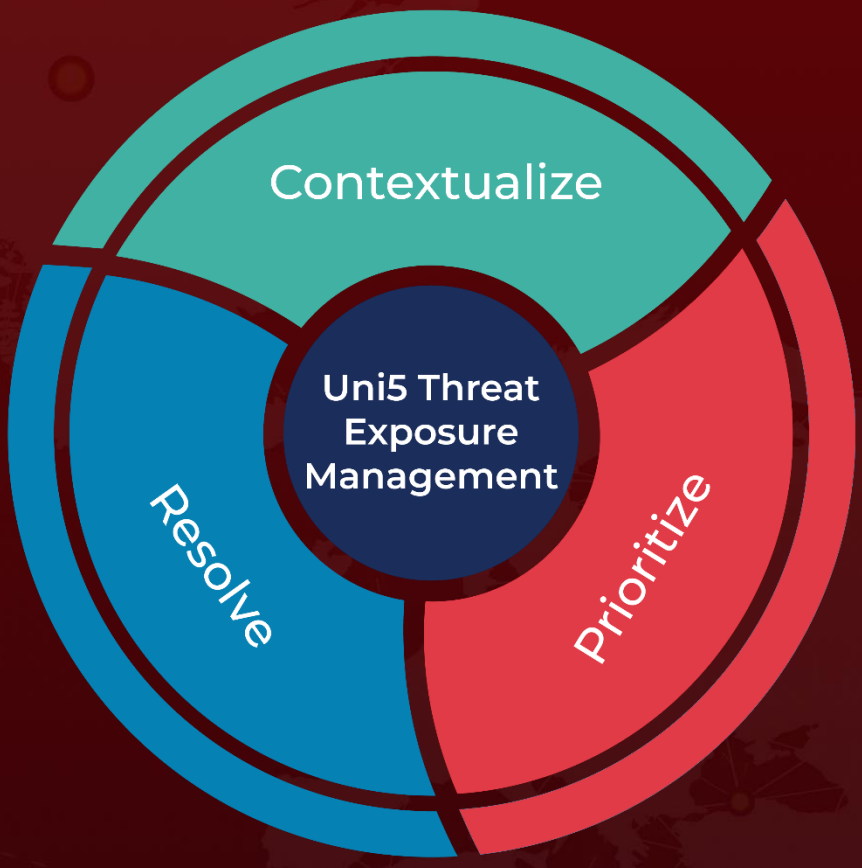
https://dashboard.shadowserver.org/statistics/iot-devices/map/?day=2024-11-14&vendor=geovision&geo=all&data_set=count&scale=log

https://github.com/FoKiiin/CVE-2024-11120

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 18, 2024 . 6:30 AM

More at www.hivepro.com