contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

GeoVision Inc. GV-Face: new CVE

CVE-2026-124600 · record published 10 November 2026

Analysis Report

Anyone running GeoVision GV-Face at version 2.2.1 must act; the record scores this 10 on CVSS 4.0, the maximum. The record names 2.2.2 as unaffected. Find which version is installed first.

PREPARED BY	NamiQ	DATE	10 November 2026
FACTS AS OF	10 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/geovision-inc-gv-face-cve-2026-124600

The bottom line

> *Anyone running GeoVision GV-Face at version 2.2.1 must act; the record scores this 10 on CVSS 4.0, the maximum. The record names 2.2.2 as unaffected. Find which version is installed first.*

At a glance

Fact	Detail
Product	GeoVision Inc. GV-Face (CVE-2026-124600)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by GV on 10 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 10 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	2.2.2 (the record names this as unaffected; no vendor advisory could be read to confirm a release date)
Who looks first	Organisations running GeoVision GV-Face at version 2.2.1. The record does not list any other version as affected.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you have GeoVision GV-Face installed anywhere?	Nothing to do for this CVE.	Check which version is running.
Is the device running version 2.2.1?	The record does not list your version as affected.	Update to 2.2.2 and review network exposure.
Can untrusted users or devices reach the same network segment as the device?	Risk is lower; still update at next maintenance window.	Prioritise updating now and isolate the device.

What it is

The device sends user credentials and authentication data over unencrypted HTTP. Anyone able to intercept traffic on the same network segment can read those credentials without needing to log in or interact with the device.

Why it matters

CWE-319 means credentials travel in cleartext HTTP — no encryption, no login needed by the interceptor. Any host on the same network segment, or at any point along the path, can capture them passively. The record scores this 10 on CVSS 4.0, the maximum. Our reading is that the risk is highest where the device sits on a shared or untrusted network; a device on a physically controlled, dedicated VLAN faces less immediate exposure, but credentials remain unprotected in transit regardless.

Things people will get wrong

- Only internet-facing devices are at risk. The record requires only the ability to intercept network traffic. A device on an internal network is still at risk if any untrusted host can reach the same segment.
- A score of 10 means remote code execution is possible. The record describes credential interception over unencrypted HTTP (CWE-319), not code execution. The score reflects the absence of any barrier to reading credentials passively.

How we would triage it

This is our judgement.

Step 1: Find the version of GV-Face you run

- Check the administration interface or device label for the firmware version. The record names 2.2.1 as affected and 2.2.2 as unaffected.

Step 2: Isolate the device from untrusted network traffic

- While preparing to patch, place the device on a VLAN or segment that only authorised hosts can reach. This reduces the window for passive credential capture.

Step 3: Update to version 2.2.2

- The record names 2.2.2 as unaffected. Apply the update following GeoVision's normal firmware update procedure. No vendor advisory could be read to supply further guidance.

Step 4: Confirm the update and review credentials in use

- After updating, confirm the version shown is 2.2.2. Consider whether credentials that passed over the device while it ran 2.2.1 should be rotated, depending on the network exposure during that period.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We have been made aware of CVE-2026-124600, which affects GeoVision GV-Face version 2.2.1. The flaw causes user credentials to be sent over unencrypted HTTP, allowing anyone on the same network to read them. The record identifies version 2.2.2 as unaffected. Please check whether we run GV-Face anywhere, confirm which version is installed, and advise on the steps needed to update to 2.2.2. We would appreciate written confirmation of the version in use and the action taken, by [date].*

The weakness behind it

The record classes this as CWE-319.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so

Network Sniffing (T1040): Capturing network traffic to read what passes.	Credential Access: stealing logins	The flaw transmits credentials in cleartext HTTP; passive capture on the same network segment would collect them directly. Network sniffing would likely be the method used.
Adversary-in-the-Middle (T1557): Sitting between two systems to read or change what they send each other.	Credential Access: stealing logins	An attacker positioned on the network path could intercept the unencrypted HTTP stream containing credentials. CWE-319 and the description both point to interception as the attack vector.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *GV-Face transmits sensitive user credentials and related authentication data over unencrypted HTTP connections. The HTTP traffic is not encrypted, an attacker with the ability to intercept network traffic.*

Versions of GeoVision Inc. GV-Face the record lists as affected:

- 2.2.1

It lists these as unaffected:

- 2.2.2

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-124600
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-124600
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- Whether versions earlier than 2.2.1 are also affected; the record lists only 2.2.1 as affected and 2.2.2 as unaffected.
- Whether HTTPS or any encrypted transport can be configured as a workaround on 2.2.1 while a patch is applied.
- What specific credential types are transmitted in cleartext — the record says 'sensitive user credentials and related authentication data' without further detail.
- The release date of version 2.2.2; no vendor advisory could be read.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 10 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-124600: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
10 November 2026	CVE record published by GV.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
GV-Face 2.2.1 on a network shared with untrusted hosts or devices	Medium	This week

GV-Face 2.2.1 on a dedicated, physically controlled access-control network	Medium	Next patch cycle
GV-Face at a version other than 2.2.1	Low	At next routine check
GV-Face already at version 2.2.2	None	None for this CVE

Appendix 4. Definition of done

- Every GeoVision Inc. GV-Face you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-124600: https://www.cve.org/CVERecord?id=CVE-2026-124600
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: dlcdn.geovision.com.tw: https://dlcdn.geovision.com.tw/TechNotice/CyberSecurity/2026/Security_Advisory_GV-Eye-2026-09-01.pdf