contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

D-Link DCS-935L: new CVE

CVE-2026-133680 · record published 20 November 2026

Analysis Report

Anyone running a D-Link DCS-935L on firmware 1.10.01 should act now: the exploit has been made public as of 20 November 2026 and no fixed firmware is listed. Restrict the camera's web interface to ...

PREPARED BY	NamiQ	DATE	21 November 2026
FACTS AS OF	21 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	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/d-link-dcs-935l-cve-2026-133680

The bottom line

> *Anyone running a D-Link DCS-935L on firmware 1.10.01 should act now: the exploit has been made public as of 20 November 2026 and no fixed firmware is listed. Restrict the camera's web interface to trusted network paths immediately, or take it offline until a patch is available.*

At a glance

Fact	Detail
Product	D-Link DCS-935L (CVE-2026-133680)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by VulDB on 20 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 21 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source we read names a fixed version
Who looks first	Anyone operating a D-Link DCS-935L IP camera on firmware 1.10.01. The record names only this firmware version and lists no unaffected releases.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a D-Link DCS-935L camera?	Nothing to do for this CVE.	Check the firmware version (next question).
Is it running firmware 1.10.01?	The record names only 1.10.01; monitor D-Link for updates on other versions.	Check whether the web interface can be reached by untrusted users.
Can anyone outside your trusted network reach the camera's web interface?	Reduce exposure anyway; no patch is yet available.	Restrict access or take it offline; check D-Link's support for a firmware update.

What it is

The record says an attacker who can reach the camera's web configuration interface can inject operating-system commands through the account or password arguments in the local recording CGI. The VulDB record states remote exploitation is possible and the exploit has been made public.

Why it matters

A score of 9.9 reflects that the flaw is in a network-reachable CGI requiring no special position to exploit. The weakness is CWE-78: a crafted account or password argument causes the device to run an OS command. The exploit has been made public, lowering the effort needed to reach any exposed camera. No fixed firmware is listed in the record. Our reading is that any DCS-935L whose web interface can be reached by an untrusted party is at material risk until a patch is available.

Things people will get wrong

- The flaw is local only, not remote The VulDB record states remote exploitation is possible; this is not a local-only flaw.
- Only firmware 1.10.01 is listed, so other versions must be safe The record names 1.10.01 as affected but lists no unaffected releases; other versions are simply not addressed by the record.

How we would triage it

This is our judgement.

Step 1: Find every DCS-935L on your network and check its firmware

- Log into each camera's administration page and note the firmware version shown; the record names 1.10.01 as the affected version.
- If direct login is not possible, ask your installer which firmware version was deployed.

Step 2: Restrict access to the camera's web interface

- Block access to the camera's web port at your perimeter firewall or router so the interface is not reachable from outside your network.
- If possible, place the camera on a network segment accessible only to authorised administrators.

Step 3: Check for a firmware update from D-Link

- The record lists no fixed firmware. Check D-Link's support pages for a DCS-935L firmware update published after 20 November 2026.
- If no update is available, consider whether the device can be taken offline until one is.

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 seen CVE-2026-133680, which affects the D-Link DCS-935L camera on firmware 1.10.01. It allows remote OS command injection through the camera's configuration interface and the exploit has been made public. No fixed firmware version has been listed. Please confirm: do we have any DCS-935L cameras installed, what firmware version are they running, and can their web interface be reached from outside our network? If we have an affected unit, please restrict its web interface access and monitor D-Link's support pages for a patch. We would like written confirmation of the firmware version and any action taken by 28 November 2026.*

The weakness behind it

The record classes this as CWE-78 and CWE-77.

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
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in a web CGI reachable over the network; exploitation would likely serve as initial access to the device. The record states remote exploitation is possible and the exploit is public.

Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	CWE-78 (OS command injection) means the injected value would likely execute as a system command on the camera; command execution would typically follow a successful exploit.
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	Embedded camera web servers typically run with elevated OS privileges; injected commands through the CGI would likely yield high-privilege access on the device.

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:

> *A vulnerability was found in D-Link DCS-935L 1.10.01. This affects the function loginRouter of the file web/cgi-bin/localrecording/setconf.cgi of the component Local Recording CGI. Performing a manipulation of the argument account/password results in os command injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.*

Versions of D-Link DCS-935L the record lists as affected:

- 1.10.01

The record gives no version ranges. Use the vendor's advisory for the affected versions.

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-2026-133680
```

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-2026-133680
```

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 D-Link has acknowledged the flaw or intends to release a patched firmware version.
- Whether the injection in the account/password arguments occurs before or after authentication is checked.
- Whether any DCS-935L firmware versions other than 1.10.01 are affected.
- What system privilege level the web CGI process holds on the camera.
- 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 21 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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-2026-133680: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:X/RC:R` 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.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
20 November 2026	CVE record published by VulDB.

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
DCS-935L on firmware 1.10.01 with its web interface reachable from the internet	Medium	immediately; no patch is available
DCS-935L on firmware 1.10.01, web interface reachable by untrusted internal users	Medium	this week
DCS-935L on firmware 1.10.01, web interface restricted to trusted administrators only	Medium	next patch cycle
No D-Link DCS-935L cameras in use	None	none for this CVE

Appendix 4. Definition of done

- Every D-Link DCS-935L 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-2026-133680: https://www.cve.org/CVERecord?id=CVE-2026-133680
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/roit-wolf/CVE/: https://github.com/roit-wolf/CVE/
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/441406
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/441406/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-133680