contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

D-Link DIR-600L: new CVE

CVE-2026-133493 · record published 20 November 2026

Analysis Report

If you run no D-Link DIR-600L router, you can stop here. If you run version 2.17b02, treat it as exposed: no fixed version is named, so restrict who can reach the device and plan a replacement now.

PREPARED BY	NamiQ	DATE	20 November 2026
FACTS AS OF	20 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/d-link-dir-600l-cve-2026-133493

The bottom line

> *If you run no D-Link DIR-600L router, you can stop here. If you run version 2.17b02, treat it as exposed: no fixed version is named, so restrict who can reach the device and plan a replacement now.*

At a glance

Fact	Detail
Product	D-Link DIR-600L (CVE-2026-133493)
Severity	Critical: 10 (CVSS 4.0)
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 20 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 running a D-Link DIR-600L on the affected firmware, especially where its web management or UPnP service can be reached from the internet or an untrusted network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a D-Link DIR-600L router anywhere?	Nothing to do for this CVE.	Check its firmware version next.
Is the firmware the one the record lists as affected?	The record names only 2.17b02; confirm your build.	Treat it as affected and reduce exposure.
Can the router be reached from the internet or an untrusted network?	Lower risk, but still plan a fix.	Act urgently; no fixed firmware exists.

What it is

The record describes command injection in the router's GENA handler, inside the gena.cgi program. It says an attacker can send a crafted request over the network and make the router run operating-system commands of their choosing. No login is mentioned.

Why it matters

The record says working exploit code is already public and scores this at the top of its scale. A command-injection flaw in a router's handler lets an attacker run their own commands on the device. Our reading is that a router sits at the edge of a network, so control of it can mean watching, redirecting or blocking the traffic of everyone behind it. With no fixed firmware named, limiting who can reach the device is the realistic defence.

Things people will get wrong

- It isn't on the exploited list, so we can leave it. The record says working exploit code is already public and rates the flaw at the top of its scale; exposure is the deciding factor here.
- A firmware update will sort it out. No source names a fixed version. Until the vendor publishes one, limiting who can reach the device is the only step available.
- A newer build near 2.17b02 is safe. The record lists 2.17b02 as affected and names no unaffected release; do not assume a nearby build is clear.

How we would triage it

This is our judgement.

Step 1: Find the devices and versions you run

- List any D-Link routers in use and read each one's model and firmware. The record lists only the DIR-600L on 2.17b02, so you need the exact build to judge each device.
- Note which of them is reachable from outside the local network, as that decides how urgent the device is.

Step 2: Reduce exposure

- Make sure the router's web management and UPnP service cannot be reached from the internet; turn off remote management where it is on.
- Limit access to the device to trusted local hosts, since the record says the attack can be launched remotely.

Step 3: Plan a fix or replacement

- No fixed firmware is named, so plan to isolate or replace an affected device rather than wait. Ask the vendor whether a firmware addressing this is coming.
- Keep checking the vendor for a release that names this flaw; a nearby build is not proof of a fix.

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 want to check our exposure to CVE-2026-133493, a remotely exploitable command-injection flaw in the D-Link DIR-600L router. Please confirm in writing whether we run any D-Link DIR-600L devices and, if so, their exact firmware version; the record lists 2.17b02 as affected. No fixed firmware has been published yet, and working exploit code is reported to be public. Please also confirm whether each device's web management and UPnP service can be reached from the internet, and disable any remote access that is not needed. Please reply with the device version and the exposure status by the end of this week.*

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 record says a crafted request can be sent remotely to the router's gena.cgi handler; exploiting such an exposed service to gain entry fits this technique.

Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The weakness is operating-system command injection, so an attacker would likely use it to run their own commands 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 identified in D-Link DIR-600L 2.17b02. Affected is the function genacgi_main of the file gena.cgi of the component GENA Handler. Such manipulation leads to os command injection. The attack can be launched remotely. The exploit is publicly available and might be used.*

Versions of D-Link DIR-600L the record lists as affected:

- 2.17b02

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-2026-133493
```

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-2026-133493
```

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 the flaw needs a login or works without one; the record does not say.
- Whether any firmware fixes it; no unaffected release is named.
- Whether other DIR-600L builds or related models are affected; only 2.17b02 is listed.
- Whether the device is still supported and will receive a fix at all; not stated.
- 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 20 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-2026-133493: 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/E:P`
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
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
A DIR-600L on the affected firmware whose admin or UPnP service faces the internet	Medium	this week

A DIR-600L on the affected firmware reachable only from the local network	Medium	next patch cycle
A D-Link router of another model or firmware build	Low	none for this CVE
No D-Link DIR-600L anywhere in the estate	None	none for this CVE

Appendix 4. Definition of done

- Every D-Link DIR-600L 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-2026-133493: https://www.cve.org/CVERecord?id=CVE-2026-133493
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/440913
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/440913/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-133493