contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# D-Link DIR-600L: new CVE

**CVE-2026-129353 · record published 14 November 2026**

## Analysis Report

Act if you run a D-Link DIR-600L router on firmware 2.17 or 2.17b02; the record says a working exploit is public. First, find whether any such router is in use and on that firmware. If you run no …

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 14 November 2026 |
| FACTS AS OF | 14 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-2026-129353

## The bottom line

> *Act if you run a D-Link DIR-600L router on firmware 2.17 or 2.17b02; the record says a working exploit is public. First, find whether any such router is in use and on that firmware. If you run no D-Link DIR-600L, you can stop here.*

## At a glance

| Fact | Detail |
|---|---|
| Product | D-Link DIR-600L (CVE-2026-129353) |
| Severity | Critical: 10 (CVSS 4.0) |
| Status | A new CVE record, published by VulDB on 14 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 14 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 home or small-office router, specifically firmware 2.17 or 2.17b02. The flaw is on the sign-in page, so a router reachable from the internet is the first to check. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run any D-Link DIR-600L router? | Nothing to do for this CVE. | Check the firmware version (next question). |
| Is its firmware 2.17 or 2.17b02? | This record does not list your version. | Check who can reach it (next question). |
| Can anyone untrusted reach its web login over the network? | Risk is limited to your own network. | Treat it as exposed and act this week. |

## What it is

The record says the router's authentication page mishandles the id and password values. A crafted value overflows a fixed-size area of memory on the stack. The record says this can be done remotely. Such an overflow can crash the device or let an attacker run code on it.

## Why it matters

This flaw is reached before any login, on the page that handles sign-in, so an attacker needs no account. The record says a working exploit is already public, which lowers the skill needed to use it. Our reading is that a small-office router often sits directly on the internet, which is where this flaw is most useful: a foothold on the device that carries all of your traffic. The record names no fixed firmware, so patching may not yet be an option, and reducing who can reach the login matters most for now.

## Things people will get wrong

- We use a strong admin password, so the overflow cannot be reached. The record says the flaw is in how the id and password values are handled, before any login succeeds; a correct password is not needed to trigger it.
- There is no patch listed, so nothing can be done yet. The record names no fixed firmware, but you can still limit who can reach the router's web login, which is where the flaw is reached.
- It is only on a vulnerability database, so it is not serious. The record says a working exploit is public and that the flaw needs no login over the network; that is worth acting on regardless of which list it is on.

## How we would triage it

This is our judgement.

## Step 1: Find which routers and firmware you run

- Identify any D-Link DIR-600L on your network and read its firmware version from the admin page, because only 2.17 and 2.17b02 are named in the record.

## Step 2: Reduce who can reach the login

- Make sure the router's web administration is not reachable from the internet, because the flaw is on the login page and the record says it can be exploited remotely.
- Restrict admin access to your local network only, since no fixed firmware is named yet.

## Step 3: Watch for a fixed firmware

- Check the vendor's support channel for a firmware update for the DIR-600L, because the record names no fixed version and one may be issued later.
- If no update appears and the device faces the internet, consider replacing it.

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.

> *Hello. We want to check our exposure to CVE-2026-129353, a stack-based buffer overflow in the D-Link DIR-600L router. Please find out whether we run any DIR-600L and, if so, which firmware version; the record names 2.17 and 2.17b02 as affected. The flaw is on the router's login page and the record says it can be exploited remotely without logging in, and that a working exploit is public. No fixed firmware is named in the record yet, so please also make sure the router's web administration is not reachable from the internet. Could you confirm in writing which version we run and what you have done to limit access, by the end of this week?*

## The weakness behind it

The record classes this as CWE-121 and CWE-119.

## 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 places the flaw on the router's internet-facing sign-in page and says it can be triggered remotely before login; exploiting such a public-facing service would typically be the way in. |

| | | |
|---|---|---|
| Endpoint Denial of Service (T1499): Crashing or overloading a single system or application. | Impact: causing damage or disruption | A stack-based buffer overflow can crash the device, so an attacker who cannot gain control would likely still be able to knock the router offline and deny service. |

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 detected in D-Link DIR-600L 2.17/2.17b02. Affected by this vulnerability is the function authenticationcgi_main of the file authentication.cgi. Performing a manipulation of the argument id/password results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used.*

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

- 2.17
- 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-2026-129353
```

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-2026-129353
```

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

- No fixed or patched firmware version is named in the record.
- The record does not say whether the flaw has been used against real devices, only that an exploit is public.
- It is not stated whether firmware other than 2.17 and 2.17b02 is affected.
- The record does not say whether disabling remote administration fully prevents the attack.
- 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 14 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-2026-129353**: 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 |
|---|---|
| 14 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 2.17 or 2.17b02 with its web login reachable from the internet | Medium | this week |

| | | |
|---|---|---|
| A DIR-600L on 2.17 or 2.17b02 reachable only from your local network | Medium | next patch cycle |
| A DIR-600L on 2.17 or 2.17b02 kept powered but no longer used | Medium | retire or isolate this week |

## 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-2026-129353: https://www.cve.org/CVERecord?id=CVE-2026-129353
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/437416
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/437416/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-129353