contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

D-Link R32: new CVE

CVE-2026-136823 · record published 25 November 2026

Analysis Report

The record scores this at 10, the maximum under CVSS 4.0, and the exploit is public. No fixed firmware is recorded; anyone running a D-Link R32 on firmware 1.10B02 should block remote access to the …

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 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-r32-cve-2026-136823

The bottom line

> *The record scores this at 10, the maximum under CVSS 4.0, and the exploit is public. No fixed firmware is recorded; anyone running a D-Link R32 on firmware 1.10B02 should block remote access to the management interface now and check for a D-Link update.*

At a glance

Fact	Detail
Product	D-Link R32 (CVE-2026-136823)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 25 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 26 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	The record lists no unaffected or fixed release. No vendor advisory page was readable. The fixed version is not known.
Who looks first	Anyone running a D-Link R32 router on firmware version 1.10B02. Those where the web management interface is reachable from outside the local network face the greatest exposure.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you use a D-Link R32 router?	Nothing to do for this CVE.	Check which firmware version it runs.
Is the firmware version 1.10B02?	The record does not list other versions as affected.	Check whether the management interface is reachable from outside your network.
Is the management interface reachable from outside your local network?	Risk is lower; monitor D-Link for a firmware update.	Restrict access now and check for a D-Link firmware update.

What it is

The record describes OS command injection in the httpd component of D-Link R32 firmware 1.10B02. An attacker who can reach the device over the network can pass a crafted value in the fpath

argument and run arbitrary commands on the router's operating system.

Why it matters

The weakness is OS command injection (CWE-78 and CWE-77), reachable over a network. The record scores this at 10, the maximum under CVSS 4.0. The exploit has been made public, meaning it requires less skill to attempt than an unpublished flaw. The record does not state whether authentication is required to reach the vulnerable endpoint, which is material: if none is needed, any device with its management interface on the internet is exposed. Our reading is that restricting remote access is the main available control until D-Link issues a fix.

Things people will get wrong

- "CVSS 4.0" means the score is below 4 out of 10 CVSS 4.0 is a framework version number, not a score. The record gives this flaw a score of 10 under that framework, which is the maximum value on the scale.
- A D-Link patch is already available The record lists no unaffected or fixed release. No vendor advisory page was readable. No fixed firmware is known from the sources available.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the firmware version on your D-Link R32

- Log in to the router's admin interface and check the firmware version shown in the system information or status section. The record names version 1.10B02 as affected.
- If you cannot access the interface directly, check documentation or records held by your IT provider.

```
cat /etc/version
```

Step 2: Restrict access to the management interface

- Disable remote management if it is enabled. The management interface should only be reachable from within your local network.

- Check that no firewall rules or port forwards expose the router's HTTP or HTTPS management ports to the internet.

Step 3: Monitor D-Link for a firmware update

- Check D-Link's support pages for a firmware update for the R32 model. The record lists no fixed version; apply any update D-Link releases for this model.
- Until a patch is available, restricting management interface access is the primary control.

Step 4: Review the device if the interface was exposed

- If the management interface was reachable from the internet while running firmware 1.10B02, review the router's logs for unexpected configuration changes or new admin accounts.
- Consider resetting to factory defaults and reconfiguring once a fix is available if there is any sign of tampering.

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 identified a security vulnerability, CVE-2026-136823, in D-Link R32 routers running firmware version 1.10B02. The record describes OS command injection reachable over the network; the exploit is public and the record scores this at 10, the maximum under CVSS 4.0. No fixed firmware is currently recorded. Please confirm whether we have any D-Link R32 devices in our environment, which firmware version each runs, and whether the management interface on any such device is accessible from outside our network. We ask for written confirmation of the firmware version and the steps planned to address this, as soon as a fix is available from D-Link.*

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 description says the attack can be initiated remotely against an httpd endpoint, which would typically indicate exploitation of a public-facing web service.
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 is OS command injection; a successful exploit would likely result in arbitrary command execution on the router's operating system.

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 R32 1.10B02. This affects an unknown function of the file /usr/bin/httpd of the component flupl self Endpoint. Performing a manipulation of the argument fpath results in os command injection. The attack can be initiated remotely. The exploit has been made public and could be used.*

Versions of D-Link R32 the record lists as affected:

- 1.10B02

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-2026-136823
```

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-2026-136823
```

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 authentication is required to reach the vulnerable endpoint on the flupl self component; the record does not say.
- Whether D-Link R32 firmware versions other than 1.10B02 are affected; the record names only that version.
- When or whether D-Link will release a fixed firmware; no vendor advisory was readable.
- Whether the vulnerable endpoint is exposed by default or requires a specific configuration to enable.
- 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 26 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-2026-136823: 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
25 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
D-Link R32 running firmware 1.10B02 with management interface reachable from the internet	Medium	Now, without waiting for a patch

D-Link R32 running firmware 1.10B02 on an internal network only	Medium	This week
D-Link R32 running a firmware version other than 1.10B02	Low	Confirm scope; monitor D-Link for updates
No D-Link R32 in the environment	None	No action for this CVE

Appendix 4. Definition of done

- Every D-Link R32 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-2026-136823: https://www.cve.org/CVERecord?id=CVE-2026-136823
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/443782
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/443782/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-136823