contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

D-Link DIR-505: new CVE

CVE-2026-120189 · record published 1 November 2026

Analysis Report

CVE-2026-120189 in D-Link DIR-505, a new record scored 10 and not on CISA's exploited list when we read it. What it is, who is affected, and what to check first.

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 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-505-cve-2026-120189

The bottom line

> *Check whether you run D-Link DIR-505. If you do, read the vendor's page for the fixed version and update. Nothing public says yet that anyone is using this flaw.*

At a glance

Fact	Detail
Product	D-Link DIR-505 (CVE-2026-120189)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 1 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 1 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 with a D-Link DIR-505 on firmware 1.10B02, and the IT provider who set it up. Check first for units reachable from the internet or from a network you do not fully trust.

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-505 anywhere, including at home offices or branches?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware version 1.10B02?	The record names only 1.10B02. Ask D-Link or your provider about other versions.	Check whether anyone untrusted can reach it.
Can the router's TFTP service be reached from the internet or an untrusted network?	Lower urgency, but plan to replace or update it.	Block that access first, then decide on replacement.

What it is

The record says a flaw in the TFTP upload filename handler of the router's tftpd program causes a stack-based buffer overflow. It can be triggered remotely. The record does not say what an attacker gains, only the overflow.

What the vendor's advisory says

We read one page on github.com. In short:

- The only source we hold is a code repository directory listing with three file names. It is not a vendor advisory.
- No source names a fixed version, a workaround or a vendor statement.

Things people will get wrong

- "It is not on the CISA list, so nobody is attacking it." The record was new when read. Absence from the list means CISA has not recorded exploitation, not that nobody is trying. The record says the exploit is public.
- "There must be a patch to install." No source we hold names a fixed version. Do not assume one exists until the vendor says so in writing.

How we would triage it

This is our judgement.

Step 1: Find the DIR-505 units and their firmware

- List every DIR-505 you own, including remote and home-office units.
- Read the firmware version in the router's admin page. The record names 1.10B02 as affected.

Step 2: Reduce exposure

- Make sure the router's TFTP service and its administration pages are not reachable from the internet.
- The record says the attack can be carried out remotely, so exposure is the main factor.

Step 3: Ask the vendor about a fix

- No source names a fixed version. Ask D-Link or your provider whether one exists, and get the answer in writing.

- If none exists, plan to replace the unit.

Step 4: Confirm the result

- Record which units were found, their versions and what was changed.
- Ask your provider to confirm in writing that no affected unit is reachable from outside.

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 are checking our exposure to CVE-2026-120189, a stack-based buffer overflow in the TFTP upload filename handler of the D-Link DIR-505, firmware 1.10B02. The record says it can be attacked remotely and that the exploit is public. Please tell us whether we run any DIR-505, where, and on which firmware. Please also confirm whether any can be reached from the internet, and whether D-Link has published a fix. Could you give us written confirmation of the versions and the action taken by the end of this week?*

The weakness behind it

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

The sources, in their words

The CVE record:

> *A vulnerability was identified in D-Link DIR-505 1.10B02. Affected is the function save_upload_file/mp_upload_file of the file /usr/bin/tftpd of the component TFTP Upload Filename Handler. The manipulation leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.*

Versions of D-Link DIR-505 the record lists as affected:

- 1.10B02

What we do not know yet

- Which firmware versions other than 1.10B02 are affected is not stated.

- No source names a fixed version or a workaround.
- The record does not say what an attacker gains beyond the overflow.
- Whether D-Link still supports this model is 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 1 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- The sections headed "Does this apply to you?", "What it is", "Exposure by situation", "Things people will get wrong", "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-2026-120189: 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
1 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-505 on 1.10B02 that faces the internet	Medium	This week, before anything else

A DIR-505 on 1.10B02 reachable only from your internal network	Medium	This week or at the next maintenance window
A DIR-505 on a version other than 1.10B02	Low	Next patch cycle, once the version's status is confirmed
No DIR-505 in your estate	None	None for this CVE

Appendix 4. Definition of done

- Every D-Link DIR-505 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-2026-120189: https://www.cve.org/CVERecord?id=CVE-2026-120189
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/Walnut1337/DIR-505_filename_rce/tree/main/poc: https://github.com/Walnut1337/DIR-505_filename_rce/tree/main/poc
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429528
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429528/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-120189