contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

D-Link DIR-878: new CVE

CVE-2026-124560 · record published 9 November 2026

Analysis Report

CVE-2026-124560 in D-Link DIR-878, 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	8 November 2026
FACTS AS OF	8 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 2.0 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-878-cve-2026-124560

The bottom line

> *Check whether you run D-Link DIR-878. 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-878 (CVE-2026-124560)
Severity	Critical: 10 (CVSS 2.0)
Status	A new CVE record, published by VulDB on 9 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 8 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No fixed version. The record states this product is no longer supported by its maintainer, and no unaffected release is listed.
Who looks first	Anyone running a D-Link DIR-878 router on firmware 1.20B05, especially where the device's management interface is reachable from outside the local 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-878 router anywhere on your network?	Nothing to do for this CVE.	Check the firmware version (next question).
Does the device show firmware version 1.20B05?	The record lists only 1.20B05 as affected; monitor for further advisories.	No patch exists; plan to isolate or replace the device (next question).
Can anyone outside your trusted network reach the router's management interface?	Reduce risk by keeping it isolated from untrusted access; prioritise replacement.	Block external access to the management interface immediately and arrange replacement.

What it is

An attacker who can reach the router's HNAP interface over a network can send a crafted request to the GetCAPTCHAsetting handler with an oversized uid value. The record says this triggers a heap-

based buffer overflow, which can allow the attacker to run code on the device remotely.

Things people will get wrong

- A score of 2.0 means this is a minor flaw. The '2.0' is the CVSS version, not the score. The record gives a score of 10, which is the maximum on CVSSv2.
- D-Link will release a patch once aware of the issue. The record explicitly states this product is no longer supported by its maintainer. No patch is expected.
- Disabling HNAP makes the device safe to keep running. The record names the HNAP handler as the entry point, but the sources do not confirm whether disabling it fully removes the attack surface on 1.20B05.

How we would triage it

This is our judgement.

Step 1: Find which DIR-878 devices you run and their firmware versions

- Log into each D-Link DIR-878 and check the firmware version shown on the status or administration page.
- The record identifies 1.20B05 as the affected version; note any device showing that string.

Step 2: Check whether the management interface is externally reachable

- Confirm whether the router's web management or HNAP interface is accessible from outside your local network.
- If it is, block that access at your perimeter immediately while you arrange the next step.

Step 3: Isolate or replace the device

- The record states the maintainer no longer supports this device; no patch will be issued, so the only remediation is replacing the hardware.
- If immediate replacement is not possible, isolate the device so that only trusted hosts can reach its management interface.

Step 4: Confirm any replacement device is not itself affected

- Verify that the replacement device or firmware does not appear in the affected ranges named in its own record.
- The record does not list any unaffected release for the DIR-878; do not assume a different firmware version on the same hardware is safe without checking its own record.

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.

The weakness behind it

The record classes this as CWE-122 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 HNAP handler is a network-facing endpoint; the record says a remote crafted request triggers the overflow, which would likely map to exploiting a public-facing application for initial access.
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	A heap-based buffer overflow in a router's CGI handler would typically allow escalation to the highest privilege level on the device if code execution is achieved.

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 DIR-878 1.20B05. This affects the function GetCAPTCHAsetting of the file bin/prog.cgi of the component HNAP Handler. Performing a manipulation of the argument uid results in heap-based buffer overflow. The attack can be initiated remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.*

Versions of D-Link DIR-878 the record lists as affected:

- 1.20B05

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-2026-124560
```

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-2026-124560
```

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

- The sources do not say whether authentication is required to reach the GetCAPTCHAsetting handler, which would affect how urgently external exposure needs to be addressed.
- No source confirms which other firmware versions, if any, are affected; the record lists only 1.20B05.
- The sources do not describe what an attacker can do after triggering the overflow, such as whether it allows persistent access or full device control.
- No source names a workaround for situations where replacing the device immediately is not possible.
- 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 8 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "Does this apply to you?", "What it is", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping" and "How we would triage it" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Timeline

Date	Event
9 November 2026	CVE record published by VulDB.

Appendix 2. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
DIR-878 on 1.20B05 with management interface reachable from the internet	Medium	Immediately
DIR-878 on 1.20B05 on a business network reachable by untrusted devices	Medium	This week
DIR-878 on 1.20B05 isolated to a small trusted network only	Medium	Next patch cycle

DIR-878 present but on a firmware version not listed as affected	Low	No immediate action needed
No DIR-878 devices on the estate	None	None for this CVE

Appendix 3. Definition of done

- Every D-Link DIR-878 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-2026-124560: https://www.cve.org/CVERecord?id=CVE-2026-124560
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/432892
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/432892/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-124560