contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

D-Link DIR-600L: new CVE

CVE-2026-133993 · record published 21 November 2026

Analysis Report

Anyone running a D-Link DIR-600L on firmware 2.17b02 should act without delay: the exploit is already public and no patched firmware is recorded. Disable UPnP on the device now and check for a …

PREPARED BY	NamiQ	DATE	22 November 2026
FACTS AS OF	22 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-2026-133993

The bottom line

> *Anyone running a D-Link DIR-600L on firmware 2.17b02 should act without delay: the exploit is already public and no patched firmware is recorded. Disable UPnP on the device now and check for a firmware update from D-Link.*

At a glance

Fact	Detail
Product	D-Link DIR-600L (CVE-2026-133993)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 21 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 22 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 router on firmware version 2.17b02, particularly where the device's UPnP or GENA handler is reachable from 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 on your network?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware version 2.17b02?	Not in the recorded affected range; monitor the vendor for further guidance.	Check whether GENA or UPnP is reachable (next question).
Is UPnP or the GENA handler reachable from untrusted networks or the internet?	Reduced exposure; still apply a patch when D-Link releases one.	Disable UPnP and restrict access to the management interface immediately.

What it is

A remotely exploitable stack-based buffer overflow in the router's GENA subscription handler lets an attacker send a crafted request to overwrite stack memory, potentially allowing them to run their

own code on the device.

Why it matters

The record gives this a score of 10 out of 10 under CVSS 4.0, the maximum. The exploit is already public, per the record. Our reading is that a maximum CVSS 4.0 score implies the attack requires no authentication and no user interaction, placing it within reach of anyone who can send a request to the device over a network. A compromised router sits at the centre of all traffic on the network, giving an attacker a position to intercept or redirect that traffic. No vendor advisory was readable and no fixed firmware is recorded.

Things people will get wrong

- If we are behind NAT, the buffer overflow cannot be reached. The record does not say which interface exposes the GENA handler. UPnP is frequently enabled on internal interfaces, so devices inside the network may be able to reach it too.

How we would triage it

This is our judgement.

Step 1: Find the firmware version on each DIR-600L

- Log in to the router's web interface and check the firmware version on the status or about page.
- If the version shown is 2.17b02, the device is within the affected range named by the record.

Step 2: Reduce exposure while no patch is available

- Disable UPnP in the router's settings if it is not actively needed; this removes the GENA handler from the reachable surface.
- Block access to the router's management and UPnP ports from untrusted networks at the network boundary.

Step 3: Watch for a firmware update from D-Link

- No fixed firmware version is recorded in the CVE record and no vendor advisory was readable at the time of this note.
- Check D-Link's support pages for the DIR-600L and apply any firmware update that addresses this flaw promptly.

Step 4: Consider replacing the device if no patch appears

- The record names no workaround beyond disabling the affected component.
- If D-Link does not issue a patch, replacing the DIR-600L with a supported device removes the exposure entirely.

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 are writing about CVE-2026-133993, a remotely exploitable stack-based buffer overflow in the D-Link DIR-600L router on firmware 2.17b02. The exploit code is already public as of 21 November 2026. We would like to know whether we run any DIR-600L devices, and if so, which firmware version they are on. No patched firmware version is recorded in the CVE record and no vendor advisory was available at that time. Please confirm in writing whether this device and firmware are present on our network, whether UPnP is enabled, and what steps are planned. We would appreciate a written response 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 flaw is in gena.cgi, a network-reachable CGI endpoint. A remotely triggered stack overflow in a web-exposed component on a public-facing device would likely be used as the initial access vector.

Adversary-in-the-Middle (T1557): Sitting between two systems to read or change what they send each other.	Credential Access: stealing logins	Gaining code execution on a router would typically position an attacker to intercept all traffic passing through it, making adversary-in-the-middle a likely follow-on outcome.

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 security flaw has been discovered in D-Link DIR-600L 2.17b02. This affects the function FUN_0040efb0 of the file gena.cgi of the component GENA Subscription Handler. Performing a manipulation of the argument service results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.*

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-2026-133993
```

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-2026-133993
```

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 before the GENA handler processes the vulnerable argument; the record does not say.
- Whether firmware versions other than 2.17b02 are also affected; the record names only that version.
- Whether D-Link has acknowledged the flaw or plans to release a patch; no vendor advisory was readable.
- Whether the vulnerable handler is exposed on the LAN interface, the WAN interface, or both.
- 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 22 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-2026-133993: 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
21 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
DIR-600L on 2.17b02 with UPnP or WAN interface reachable from the internet	Medium	This week — the exploit is already public

DIR-600L on 2.17b02 on an internal network with no external exposure	Medium	This week; monitor for a firmware update
DIR-600L on a firmware version other than 2.17b02	Low	Monitor the vendor; the record names only 2.17b02
Network running a different model or no D-Link DIR-600L at all	None	No action 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-2026-133993: https://www.cve.org/CVERecord?id=CVE-2026-133993
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/441598
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/441598/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-133993