contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

D-Link DSL-6740C: new CVE

CVE-2026-129444 · record published 15 November 2026

Analysis Report

If you use a D-Link DSL-6740C on firmware 20131126, act this week, because no source names a fixed firmware. First, make sure nobody outside your network can reach the router's FTP service. If you do …

PREPARED BY	NamiQ	DATE	15 November 2026
FACTS AS OF	15 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-dsl-6740c-cve-2026-129444

The bottom line

> *If you use a D-Link DSL-6740C on firmware 20131126, act this week, because no source names a fixed firmware. First, make sure nobody outside your network can reach the router's FTP service. If you do not use this model, you can stop reading.*

At a glance

Fact	Detail
Product	D-Link DSL-6740C (CVE-2026-129444)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 15 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 15 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 DSL-6740C router on firmware 20131126. Look first at any unit whose FTP service can be reached from the internet. Look next at units on networks shared with people you do not trust.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you have a D-Link DSL-6740C anywhere in your offices or at home workers' sites?	Nothing to do for this CVE.	Check the firmware version (next question).
Is its firmware version 20131126?	The record lists no other version. Keep an eye out for updates.	Check whether its FTP service is reachable (next question).
Is the router's FTP service on port 21 reachable from outside your network or by guests?	The risk is lower. Plan to replace the device or apply a fix if one appears.	Block it now, then plan to replace the device or apply a fix.

What it is

The record says the router's FTP service has a built-in account with a password that cannot be changed, and that it can be used over the network. A researcher's notes say this account can do anything over FTP, starting from the top folder of the device. Anyone who knows the password can log in.

Why it matters

The record gives this a score of 10. A fixed password is a key that every unit shares, and nothing about it needs to be guessed. The researcher says the FTP account can do every FTP operation from the top folder. Our reading is that someone who logs in could read the router's files and change them, which could include its settings. The record says the exploit is public. A router is the device that sits between your network and the internet, so changing it affects everything behind it.

What the vendor's advisory says

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

- These are a researcher's notes, not a vendor advisory. They say the FTP service starts by default and listens on all network interfaces without restriction.
- The researcher says the login worked on two firmware samples, S5 and N5, both Rev.A builds dated 20131126.
- The researcher also lists CWE-1391 and CWE-1188. The CVE record lists CWE-798 and CWE-259.
- The researcher says D-Link was told before publication. The notes do not mention a fix or a workaround from D-Link.
- The researcher says this is separate from another finding on the same router's web and SSH login, which uses a different default account.

Things people will get wrong

- "We changed the admin password, so we are safe." The researcher says the FTP account comes from a fixed template in the firmware. The record calls it hard-coded, and nothing suggests the admin password changes it.
- "We never turned FTP on, so it does not apply to us." The researcher says the FTP service starts by default as part of the router's normal start-up.
- "A firmware update will fix it." No source names a fixed firmware version. Do not assume a newer build fixes it unless D-Link says so.

How we would triage it

This is our judgement.

Step 1: Find the routers and versions you run

- List every D-Link DSL-6740C you use, including those at home workers' sites. The record names only this model.
- Read the firmware version on each one's status page. The record lists 20131126 as affected.

Step 2: Check whether the FTP service can be reached

- From inside the network and from outside it, check whether port 21 on the router answers. The researcher says it listens on all interfaces.

Step 3: Reduce exposure now

- Block FTP to the router from the internet and from untrusted parts of the network, using an upstream firewall if the router cannot do it.
- If you cannot block it, plan to replace the device. No source names a fix.

Step 4: Watch for a fix

- Ask D-Link or your supplier whether a fixed firmware exists for this CVE. Install it only if it names this flaw.

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 have read about CVE-2026-129444, which affects the D-Link DSL-6740C router on firmware 20131126. The CVE record says the router's FTP service has a hard-coded account that can be used over the network. Please could you tell us whether we use this router at any of our sites, and which firmware version each unit runs. Please also tell us whether its FTP service can be reached from the internet or from guest networks. As far as we know, no fixed firmware has been named yet. Please block outside access to FTP on these routers and tell us whether you advise replacing them. We would be grateful for written confirmation of the versions and of what you have done by the end of this week. Thank you.*

The weakness behind it

The record classes this as CWE-798 and CWE-259.

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
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	The record says the flaw is hard-coded credentials. An attacker would likely log in with that fixed account rather than break anything.
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 says it can be exploited remotely. The researcher says FTP listens on all interfaces, so an internet-facing router would likely be reachable directly.
Data from Local System (T1005): Copying data stored on the machine.	Collection: gathering data	The researcher says the account has full FTP permissions from the top folder. This would typically allow files on the device to be read.

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 identified in D-Link DSL-6740C 20131126. This affects an unknown function of the file /etc/templates/ftpd/ftpd_conf.php of the component FTP Daemon. Such manipulation leads to hard-coded credentials. The attack can be executed remotely. The exploit is publicly available and might be used.*

Versions of D-Link DSL-6740C the record lists as affected:

- 20131126

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-2026-129444
```

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-2026-129444
```

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 D-Link will release a fixed firmware for this model, and when.
- Whether firmware versions other than 20131126 have the same account. The record lists only that one.
- Whether turning off FTP in the router's settings, where that is possible, stops the service and closes the account.
- What the anonymous FTP account that the researcher also found in the configuration is allowed to do.
- 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 15 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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-2026-129444: 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
15 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 DSL-6740C on firmware 20131126 whose FTP service can be reached from the internet	Medium	today

A DSL-6740C on firmware 20131126 on a network with guests or shared tenants	Medium	this week
A DSL-6740C on firmware 20131126 where outside access to FTP is already blocked	Low	next replacement or patch cycle
No DSL-6740C in use	None	none for this CVE

Appendix 4. Definition of done

- Every D-Link DSL-6740C 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-2026-129444: https://www.cve.org/CVERecord?id=CVE-2026-129444
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/XueDugu/dlink-dsl6740c-ftp-default-evidence: https://github.com/XueDugu/dlink-dsl6740c-ftp-default-evidence
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/437457
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/437457/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-129444