contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

D-Link M60: new CVE

CVE-2026-125086 · record published 10 November 2026

Analysis Report

Anyone running a D-Link M60 on firmware 1.12.B01 where untrusted devices share the same network should act now — no patched version is listed in the record. First, check whether anything untrusted ...

PREPARED BY	NamiQ	DATE	10 November 2026
FACTS AS OF	10 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-m60-cve-2026-125086

The bottom line

> *Anyone running a D-Link M60 on firmware 1.12.B01 where untrusted devices share the same network should act now — no patched version is listed in the record. First, check whether anything untrusted can reach TCP port 1883 on the router and block that path at the VLAN or firewall boundary.*

At a glance

Fact	Detail
Product	D-Link M60 (CVE-2026-125086)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 10 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 10 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No unaffected or patched version is listed in the CVE record. The researcher's notes and the record name only firmware 1.12.B01; no source names a fixed release.
Who looks first	Anyone running a D-Link M60. The risk is highest in offices, shared premises, or any site where guests or untrusted devices share the same network segment. Home users where all connected devices are trusted face lower but non-zero risk.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you use a D-Link M60 router?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware version 1.12.B01?	The record names only 1.12.B01; monitor D-Link for updates.	Check whether TCP port 1883 is reachable from untrusted devices (next question).
Can untrusted devices on your network reach TCP port 1883 on the router?	Risk is contained. Watch for a firmware patch from D-Link.	Block port 1883 at the firewall or VLAN boundary immediately.

What it is

The router's mesh control service ships with a fixed credential baked into the firmware that the device rewrites on every boot. Any device on the same network that can reach TCP port 1883 can connect using that known credential and issue commands to root-privileged processes on the router.

Why it matters

The researcher's notes say the credential file is rewritten on every boot by a system daemon, so an administrator password change does not remove it. The MQTT broker is bound to all network interfaces. The researcher notes that the mesh control processes — including those handling channel assignment — run as root, and the channel-assignment process executes a shell script via a system call. Our reading is that an attacker who can reach port 1883 can send mesh control messages to root-privileged processes without needing any additional vulnerability. The record's CVSS 4.0 score is 10.

Things people will get wrong

- Changing the router's admin password removes the vulnerability. The researcher's notes say a boot-time daemon rewrites the MQTT credential file on every restart. The router's admin password is separate; changing it does not alter the MQTT broker credential.
- This only affects the router's web management interface. The flaw is in the EasyMesh MQTT broker on TCP port 1883, which the researcher confirmed listens on all interfaces. The web interface is not involved.

How we would triage it

This is our judgement.

Step 1: Find out which D-Link M60 units you have and their firmware versions

- Log in to each D-Link M60's web interface and read the firmware version on the status or information page. The CVE record names 1.12.B01 as the affected version.
- Check any network inventory or asset-management system for D-Link M60 devices and their recorded firmware.

Step 2: Check whether TCP port 1883 is reachable from untrusted segments

- From a device a guest or untrusted user could reach, test whether TCP port 1883 on the router's address is open. If it responds, the MQTT broker is reachable from that segment.
- Review firewall or managed-switch rules to confirm whether port 1883 is blocked between VLANs or between guest and corporate segments.

Step 3: Block TCP port 1883 from untrusted network segments

- Create a firewall rule or VLAN access-control entry that denies TCP port 1883 from any segment where untrusted devices connect. This reduces exposure until D-Link releases a patch.
- The researcher's notes say the broker listens on both IPv4 and IPv6 on all interfaces, so both address families must be covered.

Step 4: Apply a firmware patch when D-Link releases one

- No unaffected version is listed in the record or in any source. Monitor D-Link's firmware page for the M60 and apply any release that addresses this flaw.
- After patching, re-test that TCP port 1883 no longer accepts connections with the previously known credential.

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 a security flaw affecting the D-Link M60 router, reference CVE-2026-125086, published 10 November 2026. Firmware version 1.12.B01 ships with a fixed credential on the mesh control service at TCP port 1883 that cannot be changed and is restored on every reboot. Could you please check: whether we have any D-Link M60 routers, which firmware version they run, and whether TCP port 1883 is reachable from untrusted devices or network segments. No patched version is currently listed in the record. We would like written confirmation of the firmware version in use and whether port 1883 is blocked at the firewall or VLAN boundary, please by the end of this week.*

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 flaw is a hard-coded, publicly known credential. An attacker would likely use it to authenticate to the MQTT broker as a valid account without needing to guess or crack anything.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The researcher's notes say the channel-assignment process executes a shell script via a system call; injecting MQTT messages toward those topics would likely invoke a scripting interpreter.
Exploitation of Remote Services (T1210): Exploiting a flaw in a service on another machine to move to it.	Lateral Movement: moving to other machines	A device on the LAN or EasyMesh backhaul would exploit the MQTT service to reach root-privileged mesh control processes on the router, fitting exploitation of a remote service from within the network.

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 has been found in D-Link M60 1.12.B01. Impacted is the function system of the file /etc/emDaemon/mosquitto.conf of the component emDaemon MQTT Broker. Such manipulation leads to hard-coded credentials. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.*

Versions of D-Link M60 the record lists as affected:

- 1.12.B01

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-2026-125086
```

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-2026-125086
```

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 has acknowledged this flaw or when a patched firmware release will be available.
- Whether firmware versions other than 1.12.B01 are also affected; the CVE record and the researcher's notes name only that version.
- What mesh control actions are achievable by injecting MQTT messages; the researcher describes channel changes, member operations, and firmware download triggers but does not list the full scope.
- 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 10 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-2026-125086: 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
10 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
M60 on 1.12.B01; untrusted devices (guests, contractors) on the same VLAN as the router	Medium	Immediately — block TCP/1883 from untrusted segments now

M60 in an office or shared site with open or guest Wi-Fi	Medium	Immediately — isolate port 1883 before a patch is available
M60 at home with only trusted, known devices on the network	Medium	This week — apply a firmware patch when D-Link releases one
M60 behind a firewall that already blocks all traffic to port 1883	Low	Next patch cycle — verify the block, then patch when available
No D-Link M60 in use	None	None for this CVE

Appendix 4. Definition of done

- Every D-Link M60 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-2026-125086: https://www.cve.org/CVERecord?id=CVE-2026-125086
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/XueDugu/dlink-m60-easymesh-mqtt-credential-evid: https://github.com/XueDugu/dlink-m60-easymesh-mqtt-credential-evidence
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/433197
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/433197/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-125086