contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Qihoo 360 Whole Home Router M5: new CVE

CVE-2026-121609 · record published 4 November 2026

Analysis Report

Anyone running a Qihoo 360 Whole Home Router M5 on firmware 4.0.17.1566 should act now; no fixed version has been published and the record says the exploit is publicly available. First, confirm your …

PREPARED BY	NamiQ	DATE	5 November 2026
FACTS AS OF	5 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/qihoo-360-whole-home-router-m5-cve-2026-121609

Correction, 5 November 2026: an earlier version of this note named the M50 as an affected model as if the CVE record listed it. The record names only the M5 on firmware 4.0.17.1566; only a researcher's notes mention the M50. Treat it as reported, not confirmed.

The bottom line

> *Anyone running a Qihoo 360 Whole Home Router M5 on firmware 4.0.17.1566 should act now; no fixed version has been published and the record says the exploit is publicly available. First, confirm your firmware version and whether the device has completed initial setup.*

At a glance

Fact	Detail
Product	Qihoo 360 Whole Home Router M5 (CVE-2026-121609)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 4 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 5 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	Owners of a Qihoo 360 Whole Home Router M5 on firmware 4.0.17.1566, in particular where the device has never completed initial setup. A researcher also reports the M50 is affected; the CVE record does not list it.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Qihoo 360 Whole Home Router M5 or M50?	Nothing to do for this CVE.	Check which firmware version it is running.
Is the firmware version 4.0.17.1566?	Only this version appears in the CVE record; monitor for vendor guidance.	Check whether the device has completed its initial setup.
Is the router in factory state — has initial setup never been completed?	Risk from this specific condition is lower; still apply firmware updates when available.	Treat the device as exposed; see the steps below.

Can any untrusted device on your local network reach the router on port 23?	Exposure is contained to trusted devices; monitor and patch when available.	Prioritise restricting access or isolating the device immediately.

What it is

The router's boot script, when the device is in factory state, forces the root password to a fixed value and opens a telnet service. Anyone already on the local network can then log in as root without supplying a password of their choosing and take full control of the device.

Why it matters

The hard-coded credential and open telnet service together give full root access to anyone on the same network segment. The record states the exploit is publicly available. Root access on a home router lets an attacker read or alter all traffic the device handles. Our reading is that a guest Wi-Fi user or any other device on the LAN is sufficient to reach the service, since the source says the LAN-zone firewall accepts inbound connections. No vendor patch has been published; the researcher reports the vendor did not respond after notification on 25 September 2026.

Things people will get wrong

- Internet exposure is needed for this to be exploited The source says the WAN-side firewall rejects inbound connections but the LAN zone accepts them. Local network access — including from a guest Wi-Fi device or any connected host — is sufficient.
- The M50 is officially confirmed as affected by this CVE The CVE record lists only the M5 4.0.17.1566. A researcher's notes report the M50 carries a byte-for-byte identical script; the record does not list it.

How we would triage it

This is our judgement.

Step 1: Find the router model and firmware version

- Log in to the router's administration interface and look for the firmware or system information page; the affected version in the record is 4.0.17.1566.
- If you cannot access the admin interface, check the label on the device for the model number to confirm whether it is an M5 or M50.

Step 2: Check whether telnet is open on port 23

- If telnet is responding on port 23 of the router's LAN address, the factory-state boot script has run and the hard-coded credential is likely active.
- The source states the boot script starts telnetd only when the mptdone hardware flag is unset — that is, when initial setup has not been completed.

Step 3: Restrict access to the router's LAN interface

- Ensure that guest or IoT network segments cannot reach the router's management interface or port 23.
- Until a vendor fix is available, treat any device on the same LAN segment as a potential source of exploitation if telnet is confirmed open.

Step 4: Check for a firmware update from the vendor

- Log in to the router administration interface and check the firmware update section for any available release.
- No unaffected or fixed version has been listed in the CVE record; apply any update the vendor releases and confirm the version number has changed from 4.0.17.1566.

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 reviewing CVE-2026-121609, which affects the Qihoo 360 Whole Home Router M5 on firmware 4.0.17.1566. The flaw allows any device on the local network to gain root access via telnet when the router is in factory or uninitialized state. The exploit is reported as publicly available. No fixed firmware version has been published. Could you please confirm whether we run any 360 M5 routers, which firmware version they are on, and whether they have completed initial setup? We would like written confirmation of the current version and any steps taken or planned, by [date].*

The weakness behind it

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

The sources, in their words

The CVE record:

> *A vulnerability was identified in Qihoo 360 Whole Home Router M5 4.0.17.1566. This issue affects the function Home of the file /etc/init.d/mpt of the component Boot Script. The manipulation leads to hard-coded credentials. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Qihoo 360 Whole Home Router M5 the record lists as affected:

- 4.0.17.1566

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-2026-121609
```

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 names of running container images 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-2026-121609
```

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. It reads the names of the running images, not what is 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 a patched firmware version exists or when Qihoo 360 intends to publish one.
- Whether a device that completed initial setup is fully protected if telnetd was already started before mptdone was set.
- Whether the M50 is officially confirmed as affected by Qihoo 360.
- Whether active exploitation has occurred, given the record states the exploit is publicly available.
- 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 5 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", "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-2026-121609: 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
4 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
M5 on firmware 4.0.17.1566 in factory or uninitialized state, LAN-accessible	High	immediately
M5 on firmware 4.0.17.1566, initialization completed, LAN-accessible	Medium	this week

M50 on same firmware — a researcher reports it; the CVE record does not list it	Medium	this week
M5 on a firmware version other than 4.0.17.1566	Low	next patch cycle
No 360 M5 or M50 router in use	None	none for this CVE

Appendix 4. Definition of done

- Every Qihoo 360 Whole Home Router M5 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-2026-121609: https://www.cve.org/CVERecord?id=CVE-2026-121609
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: gist.github.com/gajgdm6-cpu/c8c3bbdeb51c076317834b41c3a919f2: https://gist.github.com/gajgdm6-cpu/c8c3bbdeb51c076317834b41c3a919f2
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/430446
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/430446/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-121609