contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

4 November 2026 · 3 new critical CVEs worth reading

Analysis Report

108 new records scored 8.5 or higher in the last 30 hours. 3 to read first, and the conditions each score leaves out.

PREPARED BY	NamiQ	DATE	4 November 2026
FACTS AS OF	4 November 2026	VERSION	1.0
TOP SCORE	Critical: 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/daily-cve-highlight-2026-11-04

The bottom line

> *All three records cover Qihoo 360 devices — two camera lines and a home router — each scoring 10, with no vendor patch and a working exploit already public. The question that sorts them: does your network include any Qihoo 360 cameras or the M5 router?*

890 CVE records were published in the last 30 hours. 108 scored 8.5 or higher. 3 are below, chosen by a fixed rule: highest score first, then fewest conditions in the wording, one product each. None is on CISA's exploited list, so a score here is the record's author describing the worst case. Read the condition before you act on the number.

At a glance

Product	Score	Fixed in	Read next
Qihoo 360 D621-2 (CVE-2026-121606)	10 (CVSS 4.0)	None. The researcher's disclosure states the flaw is present in all obtained firmware versions from 6.0.24 to 6.4.9 and that 6.4.9 remains unfixed.	Our note, below
Qihoo 360 D603-2 (CVE-2026-121607)	10 (CVSS 4.0)	None. The researcher's notes state that firmware 6.4.9 — the most recent version tested — carries byte-identical vulnerable code to earlier releases.	Our note, below
Qihoo 360 Whole Home Router M5 (CVE-2026-121609)	10 (CVSS 4.0)	See the note	Our note, below

Qihoo 360 D621-2, CVE-2026-121606

No fix exists; the analysis confirms firmware 6.4.9 remains vulnerable. Anyone running a D621-2, D603-2, D600-2, D619, D606-6, or D706 camera should isolate it from untrusted network segments now.

Score 10 (CVSS 4.0), published by VulDB on 4 November 2026. Weakness: CWE-347, CWE-345.

The firmware signature check on these cameras accepts an empty signature as valid. The record says a network-reachable attacker can push unsigned firmware and gain persistent code execution on the device. The record states no limiting condition beyond network access.

Qihoo 360 D603-2, CVE-2026-121607

No fix exists; the analysis confirms firmware 6.4.9 carries the same vulnerable code. Owners of D603-2, D600-2, D606-6, or D706 cameras should isolate the device from untrusted network segments

now.

Score 10 (CVSS 4.0), published by VulDB on 4 November 2026. Weakness: CWE-78, CWE-77.

An unvalidated host field in the camera's speed-test handler lets an attacker inject shell commands. The record says the management process runs as root, giving the attacker full device control. The record states no limiting condition beyond network access.

Qihoo 360 Whole Home Router M5, CVE-2026-121609

No fixed version is stated in the sources. If any M5 on firmware 4.0.17.1566 has not completed initial setup, isolate it from the local network immediately; otherwise confirm that setup is complete.

Score 10 (CVSS 4.0), published by VulDB on 4 November 2026. Weakness: CWE-798, CWE-259.

The router's boot script sets the root password to a fixed value and opens telnet on port 23 if initial setup is not yet complete. The record says any device on the same local network can then log in as root. Exposure depends on whether initial setup has been completed.

Fifteen minutes this morning

- List the products above you run. If none, you are done.
- For each one you run, read the version from the product and compare it to the fixed version in the table.
- If it is in range, follow the note: reduce exposure first, then update.
- Book the update, and write down who owns it and by when.

Check your own project

If you build software, you can compare what a project declares with these CVEs from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE ids leave your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-121606,CVE-2026-121607,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 ids 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-2026-121606 --cve CVE-2026-121607 --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

- These are new records. A record can change in the first days: scores, versions and wording are as at 4 November 2026. Nothing here has been tested.
- Exploitation is not recorded for any of them. That is not the same as none.
- The bottom line and the sentence under each product are our interpretation of the records and the vendors' pages, not a statement by the vendors.

Appendix 1. Severity decoded

CVE-2026-121606: 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`

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.

CVE-2026-121607: 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`

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.

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`

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	Qihoo 360 D621-2, CVE-2026-121606: record published by VulDB.
4 November 2026	Qihoo 360 D603-2, CVE-2026-121607: record published by VulDB.
4 November 2026	Qihoo 360 Whole Home Router M5, CVE-2026-121609: record published by VulDB.

Appendix 3. Definition of done

- The products above you run are listed, with versions.
- Each in range has the vendor's fixed version and mitigation noted.

- The update is booked, with an owner and a date.
- Anything not in range is recorded as checked.

Sources

- CVE record service: https://www.cve.org/
- CVE record for CVE-2026-121606: https://www.cve.org/CVERecord?id=CVE-2026-121606
- CVE record for CVE-2026-121607: https://www.cve.org/CVERecord?id=CVE-2026-121607
- CVE record for CVE-2026-121609: https://www.cve.org/CVERecord?id=CVE-2026-121609