contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Qihoo 360 D603-2: new CVE

CVE-2026-121607 · record published 4 November 2026

Analysis Report

Anyone running a Qihoo 360 D603-2, D600-2, D606-6, or D706 camera on firmware 6.4.0 to 6.4.7 should act now; no fixed version has been confirmed. Isolate the camera from untrusted networks …

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-d603-2-cve-2026-121607

Correction, 5 November 2026: an earlier version of this note named the D618_A as an affected model as if the CVE record listed it. The record does not; only a researcher's notes do. Treat it as reported, not confirmed.

The bottom line

> *Anyone running a Qihoo 360 D603-2, D600-2, D606-6, or D706 camera on firmware 6.4.0 to 6.4.7 should act now; no fixed version has been confirmed. Isolate the camera from untrusted networks immediately.*

At a glance

Fact	Detail
Product	Qihoo 360 D603-2 (CVE-2026-121607)
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 or IT providers responsible for a Qihoo 360 D603-2, D600-2, D606-6, or D706 IP camera running firmware 6.4.0 to 6.4.7. The CVE record does not list other models or versions outside that range.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Qihoo 360 D603-2, D600-2, D606-6, or D706 camera?	No action needed for this CVE.	Check the firmware version (next question).
Is the camera firmware version between 6.4.0 and 6.4.7 inclusive?	The CVE record does not list your version; monitor for vendor updates.	Assess network exposure (next question).
Can untrusted devices on your network, or the internet, reach this camera?	Risk is reduced; keep the camera on a restricted segment and monitor for a patch.	Isolate the camera from untrusted access immediately.

What it is

An attacker who can reach the camera over a network can send a crafted push message to its speed-test function. The firmware passes the host field directly into a shell command without sanitising it, so an attacker controlling that value can run arbitrary operating system commands as root on the device.

Why it matters

No authentication is required; an attacker who can reach the camera over the network can execute arbitrary commands as root. The iscm process runs as root, so there is no privilege boundary to cross. The CVE record notes the exploit has been made public. No vendor patch has been announced; a researcher's gist states that firmware 6.4.9 contains code byte-identical to the affected version, so a higher firmware number is not evidence of a fix. Our reading is that cameras reachable from untrusted networks are the most urgent concern until the vendor confirms a fix.

What the vendor's advisory says

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

- A researcher's gist (last active 10 October 2026) states no fixed version exists: firmware 6.4.9's affected function is described as byte-identical to 6.3.2. The vendor was notified on 6 October 2026 but, per the CVE record, did not respond.

Things people will get wrong

- Upgrading to firmware 6.4.9 fixes this vulnerability. A researcher's gist states that firmware 6.4.9's affected function is byte-identical to the vulnerable 6.3.2 version. The CVE record lists no unaffected release. No vendor fix has been confirmed.
- Only the D603-2 model is affected. The CVE record lists four models: D603-2, D600-2, D606-6, and D706.

How we would triage it

This is our judgement.

Step 1: Find the cameras you run and their firmware versions

- List every Qihoo 360 camera on your network; the CVE record covers D603-2, D600-2, D606-6, and D706 running firmware 6.4.0 to 6.4.7.
- Check each camera's firmware version in its administration interface or via your network management tool.

Step 2: Isolate cameras on affected firmware

- Move any camera on firmware 6.4.0 to 6.4.7 to a network segment that untrusted hosts cannot reach.
- Block inbound access to the camera's management and push-notification ports from untrusted networks.

Step 3: Monitor for a vendor patch

- No fixed version has been confirmed by the CVE record or the researcher's notes; check the vendor's firmware release page for the affected models.
- A researcher's gist reports 6.4.9 is not a fix; do not treat a firmware update as safe until the vendor names it as the fixed version for CVE-2026-121607.

Step 4: Verify isolation remains in place

- Re-confirm that firewall rules or VLAN assignments prevent untrusted hosts from reaching the camera after any network changes.

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 to ask you to check our Qihoo 360 cameras for CVE-2026-121607, an OS command-injection vulnerability affecting D603-2, D600-2, D606-6, and D706 models on firmware 6.4.0 to 6.4.7. No fixed version has been confirmed. Please check which of these models we run and the firmware version on each. If any are reachable from untrusted hosts, please isolate them immediately. We would like written confirmation of the firmware version on each camera and the steps taken, by 12 November 2026.*

The weakness behind it

The record classes this as CWE-78 and CWE-77.

The sources, in their words

The CVE record:

> *A vulnerability was found in Qihoo 360 D603-2, D600-2, D606-6 and D706 up to 6.4.9. This affects the function testspeed_command of the file /fs2/bin/iscm. Performing a manipulation of the argument host results in os command injection. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Qihoo 360 D603-2 the record lists as affected:

- 6.4.0
- 6.4.1
- 6.4.2
- 6.4.3
- 6.4.4
- 6.4.5
- 6.4.6
- 6.4.7

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-2026-121607
```

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-2026-121607
```

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 the vendor plans to release a patched firmware version, and when.
- Whether the flaw requires the camera to be connected to Qihoo's cloud push service, or whether a local network attacker alone can trigger it.
- Whether firmware versions below 6.4.0 (such as 6.3.x, which a researcher's gist reports as affected) are covered by the CVE record.
- Whether the D618_A model is affected; a researcher's gist names it, but the CVE record does not list it.
- 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-2026-121607: 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`
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
Camera firmware 6.4.0 to 6.4.7, reachable by any untrusted host or exposed to the internet	Medium	immediately

Camera firmware 6.4.0 to 6.4.7, on a restricted internal network segment only	Medium	this week
Firmware outside 6.4.0–6.4.7; researcher's gist reports 6.3.x affected but the CVE record does not list it	Medium	this week
Camera model not listed in the CVE record (D618_A is named only in a researcher's gist)	Low	next patch cycle

Appendix 4. Definition of done

- Every Qihoo 360 D603-2 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-2026-121607: https://www.cve.org/CVERecord?id=CVE-2026-121607
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: gist.github.com/gajgdm6-cpu/e8ef7f512bebb987b0119562873afd5a: https://gist.github.com/gajgdm6-cpu/e8ef7f512bebb987b0119562873afd5a
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/430444
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/430444/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-121607