contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Qihoo 360 D621-2: new CVE

CVE-2026-121606 · record published 4 November 2026

Analysis Report

Anyone running a Qihoo 360 D621-2, D603-2, D600-2, D619, D606-6, or D706 camera on firmware 6.0.24 to 6.4.9 must act now: no fix exists and the exploit is public. Isolate the camera from untrusted ...

PREPARED BY	NamiQ	DATE	4 November 2026
FACTS AS OF	4 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-d621-2-cve-2026-121606

The bottom line

> *Anyone running a Qihoo 360 D621-2, D603-2, D600-2, D619, D606-6, or D706 camera on firmware 6.0.24 to 6.4.9 must act now: no fix exists and the exploit is public. Isolate the camera from untrusted networks immediately.*

At a glance

Fact	Detail
Product	Qihoo 360 D621-2 (CVE-2026-121606)
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 4 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	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.
Who looks first	Operators of Qihoo 360 Smart Cameras on models D621-2, D603-2, D600-2, D619, D606-6, or D706. The researcher's disclosure says firmware versions 6.0.24 to 6.4.9 are all affected, including the latest available version.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Qihoo 360 Smart Camera (model D621-2, D603-2, D600-2, D619, D606-6, or D706)?	Nothing to do for this CVE.	Check the firmware version.
Is the camera's firmware version between 6.0.24 and 6.4.9 inclusive?	Nothing to do for this CVE.	No patch exists; reduce network exposure.
Can untrusted hosts — internet or internal — reach the camera's network interface?	Lower priority; monitor for a vendor firmware update.	Isolate the camera from untrusted networks now.

What it is

The firmware update handler on these cameras accepts an empty signature field as valid. An attacker who can reach the camera over the network can push unsigned firmware onto it. The record

says this enables persistent code execution on the device.

Things people will get wrong

- Updating to firmware 6.4.9 removes this risk. The researcher's disclosure states 6.4.9 is itself an affected version and that no fixed firmware exists.
- Physical access to the camera is required to exploit this. The record states the attack can be launched remotely over a network, with no authentication and no user interaction required.
- Only the D621-2 model is affected. The researcher's disclosure names six models: D621-2, D603-2, D600-2, D619, D606-6, and D706.

How we would triage it

This is our judgement.

Step 1: Identify which 360 camera models you run

- Check labels on the physical units or the mobile app's device list for model numbers D621-2, D603-2, D600-2, D619, D606-6, and D706.
- Record each model and its current firmware version, shown in the camera's admin or settings page.

Step 2: Check network exposure

- Confirm whether the camera's IP address is reachable from outside your trusted network segment — from the internet or from guest and untrusted VLANs.
- Check whether the OTA update flow can be triggered from outside the local network.

Step 3: Isolate the camera if the version is in range

- Move the camera behind a firewall rule that blocks all untrusted inbound traffic until a fixed firmware is available.
- The researcher's disclosure says no fixed version exists; updating to 6.4.9 does not resolve the flaw.

Step 4: Monitor for a vendor firmware update

- The researcher's disclosure states the vendor was notified on 6 October 2026 and did not respond. Check the Qihoo 360 support channel for any new firmware release that addresses CVE-2026-121606.

- When a patched firmware is released, apply it and confirm the version number is higher than 6.4.9.

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 operate Qihoo 360 Smart Cameras (models D621-2, D603-2, D600-2, D619, D606-6, or D706) and have become aware of CVE-2026-121606. This flaw allows unsigned firmware to be pushed to the camera over the network, with no authentication required. No fixed firmware exists; the researcher's disclosure states all versions up to and including 6.4.9 are affected. Please confirm which of these models we run, the firmware version on each, and whether any are reachable from untrusted networks. Please also isolate any affected camera from untrusted access and advise us when a patched firmware becomes available. We would like written confirmation of the firmware versions and exposure status by [date].*

The weakness behind it

The record classes this as CWE-347 and CWE-345.

The sources, in their words

The CVE record:

> *A vulnerability has been found in Qihoo 360 D621-2, D603-2, D600-2, D619, D606-6 and D706 up to 6.4.9. Affected by this issue is the function verify_sign of the file fs2/bin/iscm of the component Firmware Signature Verification. Such manipulation of the argument sign leads to improper verification of cryptographic signature. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Qihoo 360 D621-2 the record lists as affected:

- 6.4.0
- 6.4.1
- 6.4.2
- 6.4.3

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-2026-121606
```

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-2026-121606
```

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 Qihoo 360 has acknowledged the flaw or committed to a patch timeline after the researcher's disclosure.
- Whether the camera's OTA update channel can be disabled as a mitigation while no patch exists.
- Whether the firmware update interface performs any authentication before the signature check runs.
- Whether any exploitation of this flaw has been observed outside the researcher's controlled test environment.
- 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 4 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", "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-2026-121606: 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`
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 on firmware 6.0.24–6.4.9 with its network interface reachable from the internet	Medium	Immediately

Camera on firmware 6.0.24–6.4.9, reachable from untrusted internal hosts	Medium	This week
Camera on firmware 6.0.24–6.4.9, isolated to a trusted network segment	Medium	Next patch cycle; monitor for a vendor update
Camera present but firmware version not yet confirmed	Medium	Confirm version this week
None of the six affected models in use	None	None for this CVE

Appendix 4. Definition of done

- Every Qihoo 360 D621-2 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-2026-121606: https://www.cve.org/CVERecord?id=CVE-2026-121606
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: gist.github.com/gajgdm6-cpu/cf98af20ddb77f27a7c112214a6280f7: https://gist.github.com/gajgdm6-cpu/cf98af20ddb77f27a7c112214a6280f7
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/430443
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/430443/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-121606