How to secure a camera system: passwords, firmware and internet exposure

Most camera systems that get compromised were not attacked cleverly. They had a default or reused password, old firmware, and a recorder reachable from the internet. Fix those three and you have dealt with the bulk of the risk.

Networking · Published 2026-10-25 · Online version:
vuepointsecure.com/support/how-to-secure-a-camera-system-passwords-firmware-and-exposure

Cameras and recorders are internet-connected computers running firmware that many owners never update. Automated scanners look for them constantly. A compromised recorder can leak video, be enrolled in a botnet, or serve as a foothold into the rest of the network. The defence is mostly routine maintenance, done consistently.

This is a real-world problem, not a theoretical one

The US Cybersecurity and Infrastructure Security Agency (CISA) keeps a catalog of vulnerabilities known to be exploited in the wild, and camera and recorder flaws appear in it. One example is CVE-2021-36260, a command-injection flaw in the web server of some Hikvision products, added to the catalog in January 2022. Fixed firmware was available; exposed, unpatched devices were the ones at risk.

1. Passwords and accounts

- **Replace every default password**, on the recorder and on each camera. Many current devices force this at first setup; older ones and some cameras behind an NVR may not.
- **Use a long, unique password** for the admin account, stored in a password manager. Do not reuse the office Wi-Fi or email password.
- **Create separate user accounts.** Day-to-day viewers get a viewer-only account. Keep admin for configuration.
- **Secure the cloud account too.** If you use the vendor's app, the cloud login is as important as the device login. Turn on two-factor authentication where offered.
- **Remove accounts for people who have left**, including former installers.

2. Firmware

Update firmware safely

1. **Identify exact models and current versions**
   Read the model and firmware version from the device's system information page or the vendor discovery tool. Hardware revisions matter; firmware for the wrong revision can brick a device.
2. **Download only from the manufacturer**
   Use the official download center or the device's built-in online update. Never use firmware from forums or third-party file sites.
3. **Back up the configuration**
   Export the configuration file from the recorder before updating, and note channel and network settings.

4 **Update the recorder, then the cameras**
Do one device first, confirm it comes back and records, then do the rest. Do not power off a device during an update.

5 **Check the vendor's security advisories**
Most large manufacturers publish security advisories. Check them a few times a year, and after any news of a camera-related vulnerability.

> **Note**
> When a model reaches end of life and stops receiving security updates, keep it off the internet entirely, isolate it on its own network segment, and plan its replacement.

3. Internet exposure

Check	What good looks like
Port forwards on the router	None to cameras. None to the recorder unless there is no alternative. Never the admin web port (80/443) unless essential.
DMZ setting	Off, or not pointed at any camera or recorder
UPnP	Disabled on the recorder and cameras; disabled on the router if nothing needs it
Remote access method	Vendor P2P app or VPN preferred over port forwarding
External scan	An outside port check of your public IP shows no camera ports open, unless you deliberately opened them

To check, log in to the router and review its port forwarding, DMZ and UPnP pages (UPnP often has a table of ports devices opened automatically). Then test from outside as described in how to test whether a port is open. If you need remote access, compare the options in P2P cloud vs port forwarding vs VPN.

4. Network and physical

- **Segment the cameras** from office computers. See how to put cameras on their own network.
- **Turn off services you do not use**, such as Telnet or SSH, and RTSP or ONVIF if no third-party software needs them.
- **Set the correct time and time zone** (NTP) so recordings and logs are usable as evidence.
- **Lock up the recorder.** Physical access to the NVR means access to the footage and often a password reset path.
- **Protect exposed cable runs and outdoor switch boxes** so a camera's network port cannot be used to plug into your network.

> **Once-a-year checklist**
> Review user accounts. Update firmware. Re-check router forwards, DMZ and UPnP. Run an external port check. Confirm recordings and time are correct. Twenty minutes, once a year, covers most of what goes wrong.

Frequently asked questions

Is a camera system safe if I only use the manufacturer's app?

It is much safer than port forwarding because nothing is opened inbound. You still need strong unique passwords on the device and the cloud account, two-factor authentication where available, and current firmware.

Should I replace cameras from a particular brand for security reasons?

It depends on your obligations. US federal rules restrict some brands for certain buyers, and end-of-life models no longer get fixes. For everyone else, patched firmware, no inbound exposure and segmentation matter more than the logo.

How do I know if my recorder has already been compromised?

Warning signs include unknown user accounts, changed settings or passwords, unexpected reboots, and unfamiliar entries in the device log. If you see these, disconnect it from the internet, reset it to factory defaults, update firmware and set new credentials before reconnecting.

Related guides

- P2P cloud vs port forwarding vs VPN for remote viewing — vuepointsecure.com/support/p2p-cloud-vs-port-forwarding-vs-vpn-for-remote-viewing
- How to put cameras on their own network (VLAN) — vuepointsecure.com/support/how-to-put-cameras-on-their-own-network-vlan
- How to test whether a port is open — vuepointsecure.com/support/how-to-test-whether-a-port-is-open
- What the FCC rules on Chinese cameras mean for your next job — vuepointsecure.com/support/chinese-camera-fcc-rules
- All support articles — vuepointsecure.com/support

Need help with a site? Call (888) 203-2260 or visit vuepointsecure.com/contact. Menu names and defaults vary by model and firmware; check your device's documentation.