contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Check Point Multiple Products exploited

CVE-2026-123039 · on CISA's exploited list since 13 November 2026

Analysis Report

Owners of Check Point Quantum Security Gateway or Quantum Security Management are already past CISA's 16 November 2026 date. Find which Jumbo Hotfix Take each system runs today, then apply the ...

PREPARED BY	NamiQ	DATE	18 November 2026
FACTS AS OF	18 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 7.8**	STATUS	On CISA's exploited list; due 16 November 2026

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/check-point-multiple-products-cve-2026-123039

The bottom line

> *Owners of Check Point Quantum Security Gateway or Quantum Security Management are already past CISA's 16 November 2026 date. Find which Jumbo Hotfix Take each system runs today, then apply the vendor's mitigations. If you run neither product, you can stop reading.*

At a glance

Fact	Detail
Product	Check Point Multiple Products (CVE-2026-123039)
Severity	High: 7.8 (CVSS 3.1)
CISA	On its exploited list since 13 November 2026. Deadline for US federal agencies: 16 November 2026.
Chance of exploitation (EPSS)	0.02, the estimated chance in the next 30 days, as at 18 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	No source we read names a fixed version
Who looks first	Firms and providers that run Quantum Security Gateway or Quantum Security Management on R81.20, R82, R82.10 or R82.20, especially where anyone other than a trusted administrator can log in to the device.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Check Point Quantum Security Gateway or Quantum Security Management?	Nothing to do for this CVE.	Check the release and Jumbo Hotfix Take (next question).
Is a system on R81.20, R82, R82.10 or R82.20 at or below the Take the record lists?	Not in the listed ranges. Keep a written record of the Take.	Treat it as affected and apply the vendor's mitigations.
Can anyone other than trusted administrators log in to the device, by shell or any account?	The attacker's first step is blocked. Still mitigate on the vendor's timetable.	Raise priority: any such account could gain root.

Could a stolen or shared low-privilege account reach the device from the network?	Risk is lower. Keep the account list short and reviewed.	Remove or restrict those logins first, then apply the mitigations.

What it is

The record says a Gaia OS service that runs as root listens on a local socket that any user can write to, and it does not check who connects. A user who is already logged in on the device can send a command and have it run as root.

Why it matters

Our reading is that this flaw is no use to an outsider on its own, because the attacker must already be logged in. Its value is as a second step. A stolen low-privilege account, or a contractor login, becomes root on a device that enforces or manages network rules. The score of 7.8 understates that, because the target is a security device. Root there may let an attacker change rules, read stored settings or hide their tracks.

Things people will get wrong

- "This needs no login, so it is an internet-facing emergency." The record says the attacker must be an authenticated local user. The risk lies in who can log in, not in an open port.
- "It only matters for gateways." The record lists both Quantum Security Gateway and Quantum Security Management, in the same four release ranges.
- "We are on R82, so we are covered." R82 is listed up to Jumbo Hotfix Take 130. The Take decides it, not the release name.

The wording includes conditions the score may not show: the attacker must be logged in. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find the release and Take on each system

- List every Check Point gateway and management server, and note the release and Jumbo Hotfix Take.
- Compare each with the four ranges the record lists. Anything at or below the listed Take is affected.

Step 2: Reduce who can log in

- List the accounts that can open a shell on each device. Remove or lock any that are not needed.
- The flaw needs a logged-in user, so fewer accounts means fewer ways to use it.

Step 3: Apply the vendor's mitigations

- CISA's required action is to apply the vendor's mitigations. We could not read a vendor page, so ask your provider or Check Point for the exact instructions.
- No source names a fixed Take, so do not assume a newer Take fixes it until the vendor says so.

Step 4: Get written confirmation and review logs

- Ask for the Take and the mitigation status of each system in writing.
- Review recent logins and root activity on affected systems, as described under what to look for.

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. CISA's wording adds that you should stop using the product if no mitigation is available.

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 need to check our exposure to CVE-2026-123039 in Check Point Quantum Security Gateway and Quantum Security Management. The record says a local user on Gaia OS can run commands as root. Please tell us whether we run either product, on which systems, and which release and Jumbo Hotfix Take each uses. Please also tell us who can log in to them. CISA's date for this flaw was 16 November 2026. Please apply the vendor's mitigations and send written confirmation of each Take and the mitigation status by a date you suggest, ideally this week. If you know of a fixed Take, please name it.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Logins by non-administrator or rarely used accounts on affected devices, especially shell sessions.

- Commands run as root soon after such a login, or by a process that user started.
- Unexpected new accounts or changed settings on the device after a low-privilege login.

The weakness behind it

The record classes this as CWE-862 (Missing Authorization) and CWE-732 (Incorrect Permission Assignment for Critical Resource).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	The record says a logged-in local user can run a command as root, so this would likely be used to move from a low-privilege account to full control of the device.
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	The attacker must already hold a valid login, so a stolen or shared account would likely be the first step before the flaw is used.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Check Point Firewall, Multi-Domain Security Management Server, Scalable Platforms, Security Gateway, and Security Management Server contain an incorrect permissions assignment for critical resources vulnerability when the Gaia OS DynamicCLI daemon runs as root and listens on a world-writable local socket without authenticating connecting processes. An authenticated local user can send a command to the socket and have it executed as root.*

The CVE record, published by Checkpoint on 12 November 2026:

> *The Gaia OS DynamicCLI daemon runs as root and listens on a world-writable local socket (/tmp/dynamic_socket) without authenticating connecting processes. An authenticated local user can send a command to the socket and have it executed as root.*

Versions of checkpoint Quantum Security Gateway the record lists as affected:

- R82.10 with Jumbo Hotfix Take 50 or below
- R82.20 with Jumbo Hotfix Take 10 or below
- R82 with Jumbo Hotfix Take 130 or below
- R81.20 with Jumbo Hotfix Take 173 or below

Versions of checkpoint Quantum Security Management the record lists as affected:

- R82.10 with Jumbo Hotfix Take 50 or below
- R82.20 with Jumbo Hotfix Take 10 or below
- R82 with Jumbo Hotfix Take 130 or below
- R81.20 with Jumbo Hotfix Take 173 or below

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

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-2026-123039
```

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 hardware (maker, model, firmware), the running container images with their operating system and packages, 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-2026-123039
```

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. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages 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

- Which Jumbo Hotfix Take, if any, fixes the flaw: the record lists only affected ranges, and no vendor page was readable.
- What the vendor's mitigation consists of in practice, and whether it removes the flaw or only reduces exposure.
- Whether other Check Point products or releases are affected: the record names only the two products above.
- How the flaw has been used in attacks: the sources give no detail.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 18 November 2026; the vendor's advisory wins where it differs.
- 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", "Likely ATT&CK mapping", "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-2026-123039: score 7.8, `CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Local	Needs an account or code already running on the machine.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
12 November 2026	CVE record published by Checkpoint.
13 November 2026	CISA added it to its list of exploited vulnerabilities.
16 November 2026	CISA's deadline for US federal agencies.

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
Affected Take, and non-administrators or shared accounts can log in	High	Now; CISA's date has passed
Affected Take, logins limited to a few trusted administrators	Medium	This week
Management server on an affected Take, reachable only from an admin network	Medium	This week

Version above the listed Take, or a different release	Low	Confirm the Take in writing; then none
You do not run Check Point products	None	none for this CVE

Appendix 4. Definition of done

- Every Check Point Multiple Products you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-123039: https://www.cve.org/CVERecord?id=CVE-2026-123039
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: support.checkpoint.com: https://support.checkpoint.com/results/sk/sk1000362