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

Act only if you run Check Point. It is on CISA's list, due 16 November 2026. First, find whether you run Quantum Security Gateway or Quantum Security Management on the listed Jumbo Hotfix levels; if ...

PREPARED BY	NamiQ	DATE	14 November 2026
FACTS AS OF	14 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

> *Act only if you run Check Point. It is on CISA's list, due 16 November 2026. First, find whether you run Quantum Security Gateway or Quantum Security Management on the listed Jumbo Hotfix levels; if you run no Check Point gear, you can stop here.*

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 14 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	Anyone running Check Point Quantum Security Gateway or Quantum Security Management on R82.10, R82.20, R82 or R81.20 at the Jumbo Hotfix Takes the record lists, where people other than full admins can log in.

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 hotfix level next.
Is it R82.10, R82.20, R82 or R81.20 at the listed Jumbo Hotfix Take or below?	Not in the affected range for this CVE.	Treat it as affected; see who can log in.
Can anyone other than trusted admins log in to the appliance?	Lower risk, but still patch in the window.	Higher risk; prioritise the fix.

What it is

A user who is already logged in to the device can send a command to a local socket that a system service runs as root. The record says this gives them root — full control of the firewall or management server — from an ordinary account.

Things people will get wrong

- This is a remote attack, so we must take the firewall offline now. The record says the attacker must already be logged in. It is local privilege escalation, not a network break-in.
- We are on the latest Jumbo Hotfix, so we are safe. No source here names a fixed Take. The record lists only Takes that are affected. Confirm with Check Point which Take resolves it.
- It is only 7.8, not critical, so it can wait. It lets any account become root on a security device; given the short deadline, patch promptly rather than defer it.

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.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find what you run and its hotfix level

- List your Check Point products, versions and the Jumbo Hotfix Take on each, to see if any match the affected R82.10, R82.20, R82 or R81.20 levels in the record.

```
show version all
show installer packages installed
```

Step 2: Limit who can log in

- The attack needs a logged-in account, so remove or tighten non-admin local logins and shell access to the appliance while you arrange the fix.

Step 3: Apply the vendor's fix

- Apply the fix in line with Check Point's instructions. No source here names the Take that fixes it, so confirm the correct Jumbo Hotfix with the vendor before you rely on it.

Step 4: Check for misuse if exposed

- Look for unexpected commands run as root or access to the local socket, and for accounts or changes you cannot account 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.

> *Hello, we need your help with a security issue. A vulnerability, CVE-2026-123039, affects Check Point Quantum Security Gateway and Quantum Security Management. Please confirm whether we run either product, where, and on which version and Jumbo Hotfix Take. The record lists R82.10, R82.20, R82 and R81.20 at certain Take levels as affected; a logged-in user could gain root on the device. CISA has set a deadline of 16 November 2026. No public source here names the fixed Take, so please check with Check Point which Jumbo Hotfix resolves it. Could you reply in writing with the version we run and your plan to fix it by 16 November 2026? Thank you.*

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:

- Commands or processes running as root that you cannot tie to normal admin work.
- Access to the local socket the service listens on from ordinary user accounts.
- New accounts, configuration changes or logins by non-admin users you cannot account for.

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
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 record says the attacker must already be logged in, so a valid local account on the appliance would likely be the starting point.
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 command sent to the socket runs as root, which would typically let a low-privilege user raise their privileges to full control.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The flaw works by sending a command that the root service then executes, so running commands through that interface is the likely mechanism.

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

- No source here names the Jumbo Hotfix Take that fixes this flaw.
- No workaround or mitigation detail is recorded beyond applying the vendor's fix.
- CISA names more products, such as Multi-Domain Security Management and Scalable Platforms; the record lists only Quantum Security Gateway and Quantum Security Management.
- The sources do not say whether the vulnerable socket is reachable in a default configuration.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 14 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "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
A management server on an affected Jumbo Hotfix level that several staff accounts can log in to	High	Within CISA's window
A gateway on an affected level with local accounts beyond full admins	Medium	Within CISA's window
An affected appliance only trusted admins can log in to	Medium	This patch cycle

No Check Point products in your estate	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