CISA Flags Check Point Gaia OS Flaw Allowing Local Root Command Execution (CVE-2026-123039)



CISA lists CVE-2026-123039, a permissions flaw in the Gaia OS DynamicCLI daemon across several Check Point products. An authenticated local user can run commands as root. Apply vendor mitigations.

- CVE-2026-123039 is an incorrect permission assignment for a critical resource.
- Affected: Check Point Firewall, Multi-Domain Security Management Server, Scalable Platforms, Security Gateway and Security Management Server.
- The Gaia OS DynamicCLI daemon runs as root and listens on a world-writable local socket without authenticating callers.
- An authenticated local user can send a command to the socket and have it executed as root.
- CISA requires vendor mitigations, with a federal due date of 2026-11-16.

CISA has added CVE-2026-123039 to its list of vulnerabilities requiring action. It affects several Check Point products: Firewall, Multi-Domain Security Management Server, Scalable Platforms, Security Gateway and Security Management Server.

What the flaw is

The Gaia OS DynamicCLI daemon runs as root and listens on a local socket that any local account can write to. It does not authenticate the processes that connect. As a result, an authenticated local user can send a command to the socket and have it executed with root privileges.

The source describes a local attack path. It requires an account on the device, but the outcome is full administrative control of a security appliance, which makes the issue relevant to any organisation that relies on these products at its network perimeter or for central management.

What CISA asks for

CISA directs organisations to apply mitigations according to the vendor's instructions, in line with its BOD 26-04 guidance on prioritising security updates by risk and its forensics triage requirements. Where mitigations are unavailable, the guidance is to follow the applicable BOD 26-04 provisions for cloud services or stop using the product. Each organisation is responsible for assessing the internet exposure of its assets. The federal due date is 2026-11-16.

Practical view

Saudi institutions are not bound by BOD 26-04, but it is a sensible benchmark. The priority is to identify affected Check Point systems, apply the vendor's mitigations, and review who holds local access to them.

What to do now

1. Inventory all Check Point Firewall, Security Gateway, Security Management Server, Multi-Domain and Scalable Platforms systems running Gaia OS.
2. Apply the mitigations in the vendor's instructions, starting with internet-exposed and management systems.
3. Review and restrict local and shell access accounts on these appliances to those strictly needed.
4. Check logs and account activity on affected devices for unexpected local commands or privilege changes, and preserve evidence if anything is found.
5. Record the decision and timeline in your vulnerability management process under NCA ECC and SAMA CSF requirements.