GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

16 November 2026

Advisory 377: Check Point Gaia OS DynamicCLI Privilege Escalation Vulnerability (CVE-2026-123039).

Release Date: 13th November 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-123039 is a privilege escalation vulnerability (CWE-862 and CWE-732) in Gaia OS, the operating system of Check Point firewalls and management servers. The DynamicCLI daemon runs as root and listens on a world-writable local socket (/tmp/dynamic_socket) without checking which process is connecting. Any low-privileged local user or service account can send a command to this socket and have it run as root.

What are the systems affected?

The vulnerability affects Check Point Gaia OS on Force Firewalls (Security Gateways), Management and Log Servers, Multi-Domain Security Management and Multi-Domain Log Server, and Maestro Orchestrator:

- R82.20 with Jumbo Hotfix Take 10 or below
- R82.10 with Jumbo Hotfix Take 50 or below
- R82 with Jumbo Hotfix Take 130 or below
- R81.20 with Jumbo Hotfix Take 173 or below
- R81.10 and R81 (end of support, no fixed take listed)

- Gateways with Mobile Access, SSL Network Extender, SAML VPN, Identity Awareness Captive Portal, UserCheck or Zero Phishing portals are at the highest risk, because PHP2Shell gives attackers the first foothold

Not affected / patched version (November Jumbo Hotfix Accumulator, which also includes the PHP2Shell fix):

- R82.20 Take 14 or later
- R82.10 Take 52 or later
- R82 Take 132 or later
- R81.20 Take 174 or later
- Quantum Spark appliances and Smart-1 Cloud are not affected by CVE-2026-123039, but Spark is affected by PHP2Shell and should run the latest GA release

What does this mean?

Successful exploitation may allow attackers to:

- Take full root control of the firewall or management server
- Install a persistent backdoor that survives patching
- Read or change firewall policy, VPN settings and stored credentials
- Move from the firewall into the internal network, including virtualisation hosts
- Destroy data and systems, as seen in wiper attacks against VMware ESXi hosts

Mitigation process

CERTVU recommends the following:

1. Install the November Jumbo Hotfix
Install the fixed Jumbo Hotfix take listed above on all Management Servers and Security Gateways, starting with gateways whose Mobile Access or other portals face the internet. Check the installed take with "show version all" in Clish or "cpinfo -y all" in Expert mode. The October PHP2Shell hotfix alone does not fix CVE-2026-123039.

2. Replace end-of-support releases
R81 and R81.10 have no fixed take. Apply the sk1000362 mitigation and plan an upgrade to a supported release with a fixed take.

Reference

1. https://support.checkpoint.com/results/sk/sk1000362
2. https://support.checkpoint.com/results/sk/sk1000302
3. https://www.cve.org/CVERecord?id=CVE-2026-123039
4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-123039
5. https://www.cisa.gov/news-events/alerts/2026/11/13/cisa-adds-two-known-exploited-vulnerabilities-catalog