CYBER ADVISORY

Thursday, July 23, 2026 **CAL-CSIC-202607-A-013**

Critical Improper Authentication Vulnerability Idenified in Check Point SmartConsole

Unauthenticated Remote Attacker	Policy Modification	Configuration Modification	Mitigation Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical improper authentication vulnerability within Check Point's SmartConsole login process. SmartConsole is a key component in Check Point's architecture, serving as the primary management interface for administrators to configure policy, monitoring logs, compliance and audit reporting, user management, and threat prevention configuration.[1] CVE-2026-16232 carries a CVSS 3.1 score of 9.1.[2]

CVE-2026-0770 is an improper authentication vulnerability that enables an unauthenticated remote attacker to obtain an application token and use it to authenticate with full administrative privileges. Successful remote exploitation is conditional, however. Internet access to the Management Server IP address is required, and no restrictions on Trusted Clients (GUI clients) have to be enabled. Successful exploitation allows the now authenticated attacker to modify security policy and configurations.[3]

Check Point has acknowledged active exploitation on a small number of clients and has issued a security update that includes hotfixes with mitigation instructions for CVE-2026-16232.[4] Check Point has also released the following IOCs to look for within SmartConsole's Logs and Monitor feature:

1. 151.241.99[.]207
2. 151.241.99[.]233
3. 158.62.198[.]182
4. 192.142.10[.]99
5. 139.28.37[.]250

The Cal-CSIC recommends following the Check Point update guidance as soon as possible. If patching cannot be immediately accomplished utilize the following workaround until the vendor hotfix can be completed:

1. Limit Trusted Clients (GUI Clients) to trusted IP addresses/subnets
2. Follow the Check Point Hardening Best Practices Guide.[5]

For additional details regarding CVE-2026-16232, please use this link:

Check Point Security Update: https://support.checkpoint.com/results/sk/sk185169/

Affected Products and Versions

Product	Affected Version
Security Management	R81.10 R81.20 R82 R82.10 *All previous versions are also impacted*
Multi-Domain Management	

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] HacktheForum; "What is the role of the Smart Console in Check Point's architecture"; https://www.hacktheforum.com/checkpoint-firewall/what-is-the-role-of-the-smart-console-in-check-points-architecture/; accessed 23 July 2026

[2] NVD; "CVE-2026-16232 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-16232; accessed 23 July 2026

[3] Check Point Support Center; "Langflow < 1.3.0 - Remote Code Execution via validate_code exec() (CVE-2026-0770)"; https://pentest-tools.com/vulnerabilities-exploits/langflow-130-remote-code-execution-via-validate-code-exec_28889; accessed 22 July 2026

[4] Check Point Support Center; "Langflow < 1.3.0 - Remote Code Execution via validate_code exec() (CVE-2026-0770)"; https://pentest-tools.com/vulnerabilities-exploits/langflow-130-remote-code-execution-via-validate-code-exec_28889; accessed 22 July 2026

[5] Hybrid Mesh Network Security; "Check Point Gateway and Management Hardening"; https://sc1.checkpoint.com/documents/Check_Point_Gateway_and_Management_Hardening/CP_Check_Point_Gateway_and_Management_Hardening.pdf; accessed 23 July 2026