Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Check Point SmartConsole Authentication Bypass Exploited

Date of Publication	Admiralty Code	TA Number
July 24, 2026	A1	TA2026211

Summary

First Seen: Prior to July 22, 2026
Affected Products: Check Point Security Management Server, Check Point Multi-Domain Security Management Server (MDS)
Impact: Check Point has patched a critical flaw in SmartConsole, the admin panel used to manage its Security Management and Multi-Domain Security Management (MDS) servers. Tracked as CVE-2026-16232, the flaw is an authentication bypass in the login process that lets an unauthenticated remote attacker grab a valid application login token and use it to log in with full administrator rights, without any password. Check Point found the bug during a routine internal review and confirmed it was already being exploited against a small number of customers before a fix existed. Exploitation only works when the Management Server is reachable from the internet and does not restrict Trusted Clients (GUI clients).

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-16232	Check Point SmartConsole Improper Authentication Vulnerability	Check Point Security Management / Multi-Domain Security Management	✓	✓	✓

Vulnerability Details

#1 CVE-2026-16232 is classified as improper authentication (CWE-287. The weakness lives in the SmartConsole login process, the workflow responsible for authenticating administrators to a Check Point Security Management or Multi-Domain Security Management server.

#2 Rather than requiring valid credentials, the flawed login flow can be manipulated into handing an application login token to an unauthenticated party. That token is a trusted piece of authentication material, so once an attacker holds it, they can present it back to the management server and be treated as a fully authenticated administrator. In effect, the bug converts an anonymous network connection into an admin session without ever cracking or phishing a password.

#3 The attack is remote and network-based, but it is gated by configuration. Successful exploitation requires the Management Server's IP address to be reachable over the internet and the Trusted Clients (GUI clients) setting to leave connecting hosts unrestricted.

#4 The vulnerability spans a wide range of releases of the Security Management Server and Multi-Domain Security Management Server, including R77.30, R80, R80.10, R80.20, R80.30, R81, R81.10, R81.20, R82, and R82.10. Fixes are delivered through Jumbo Hotfix Accumulators: R82.10 from Take 36, R82 from Take 118, and R81.20 from Take 158. The older, largely end-of-support branches (R81.10, R81, R80.30, R80.20, R80.10, R80, and R77.30) have no specified fix, so organizations still running them must lean on mitigation and upgrade planning.

#5 Check Point has confirmed active exploitation. According to the vendor, the issue surfaced during a routine internal review, and follow-up analysis showed that CVE-2026-16232 had been exploited, affecting a small number of customers who have since been notified.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-16232	Check Point Security Management Server/ Multi-Domain Security Management (R77.30, R80, R80.10, R80.20, R80.30, R81 R81.10, R81.20, R82, R82.10)	cpe:2.3:a:checkpoint:multi-domain_security_management:*:*:*:*:*:*:*:*	CWE-287

Recommendations

Patch Affected Management Servers Immediately: Install the latest Jumbo Hotfix Accumulator for your release without waiting for a routine maintenance window, using Take 36 or later for R82.10, Take 118 or later for R82, and Take 158 or later for R81.20. This is the only step that removes the underlying flaw, and every other measure below merely reduces exposure until the hotfix is in place.

Restrict Trusted Clients and Management Exposure: For environments where the hotfix cannot be applied at once, limit Trusted Clients (GUI clients) to specific trusted IP addresses or subnets rather than allowing "Any," place management access behind a firewall that only permits authorized IP addresses, and confirm that implied rules for control connections are enabled. Following the Check Point Hardening Best Practices Guide shrinks the attack surface, though it does not close the vulnerability itself.

Upgrade End-of-Support Versions: Organizations running R81.10, R81, R80.30, R80.20, R80.10, R80, or R77.30 have no vendor fix for this CVE, so plan a migration to a supported release that can receive the Jumbo Hotfix. In the interim, the mitigation steps above are the primary line of defense for these deployments.

Hunt for Signs of Compromise: Treat any internet-exposed management server as potentially targeted and investigate even after patching. In SmartConsole, review Logs & Monitor / Logs & Events for traffic to or from the published attacker IP addresses, and search the Audit Logs view for events where the authentication method is an application token. Also examine administrator, SmartConsole, API, and application-token activity for anything unexpected, keeping in mind that the absence of the known indicators does not prove an environment was untouched.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Defense Evasion	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
	T1562: Impair Defenses	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	151[.]241[.]99[.]207, 151[.]241[.]99[.]233, 158[.]62[.]198[.]182, 192[.]142[.]10[.]99, 139[.]28[.]37[.]250

Patch Link

https://support.checkpoint.com/results/sk/sk185169/

References

https://support.checkpoint.com/results/sk/sk185169/

https://sc1.checkpoint.com/documents/Check_Point_Gateway_and_Management_Hardening/CP_Check_Point_Gateway_and_Management_Hardening.pdf

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 24, 2026 • 07:30 AM

More at www.hivepro.com