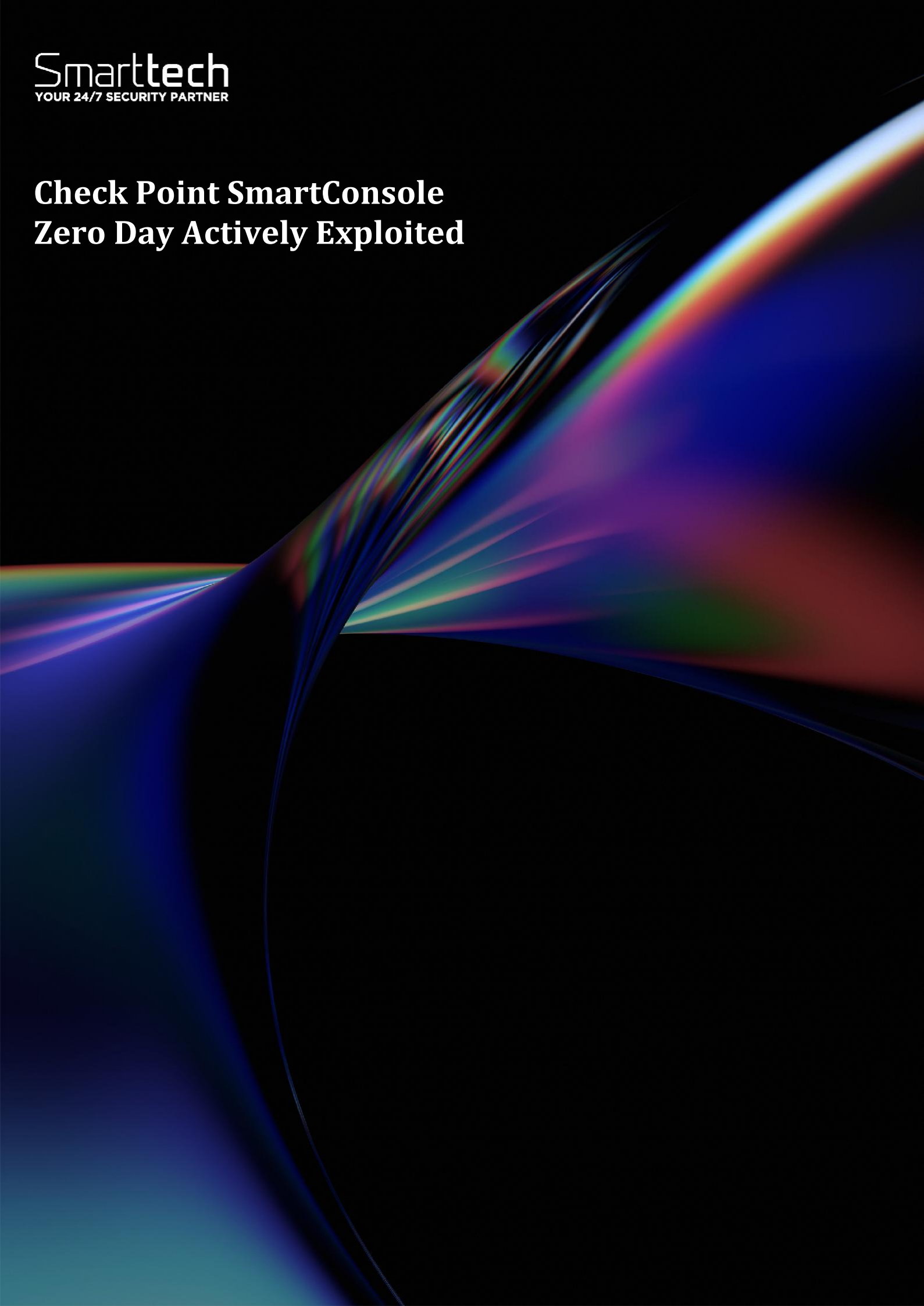


Check Point SmartConsole Zero Day Actively Exploited



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	124
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-07-23
Issue Date	2026-07-23

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

A critical vulnerability in Check Point's SmartConsole graphical user interface (GUI) is being actively exploited in the wild. Tracked as CVE-2026-16232, the flaw stems from an authentication bypass vulnerability in Check Point Security Management Server and Multi-Domain Security Management Server (MDS) that allows unauthenticated attackers to obtain a valid application login token and authenticate with administrator privileges. Successful exploitation could allow the attackers to modify security policies and security configurations.

Risk:

Government:

- Large and medium government entities: Critical
- Small government entities: Critical

Businesses:

- Large and medium business entities: Critical
- Small business entities: Critical

Technical summary:

CVE	Description
CVE-2026-16232 CVSS Score: 9.3 Improper Authentication	An authentication bypass vulnerability in the Check Point SmartConsole login process allows an unauthenticated remote attacker to obtain an application login token and use it to authenticate with full administrative privileges. Remote exploitation requires internet access to the Management Server IP address and a configuration that does not restrict Trusted Clients.

Affected Products:

Product	Version
Security Management Server, Multi-Domain Security Management Server (MDS)	R77.30, R80, R80.10, R80.20, R80.30, R81 R81.10, R81.20, R82, R82.10

Identifying an attack:

- In SmartConsole, go to Logs & Monitor / Logs & Events, and search for events where either the source IP or destination IP matches one of the known attacker IP addresses.
 - Attacker IP addresses (IoCs):
 - 151.241.99.207
 - 151.241.99.233
 - 158.62.198.182
 - 192.142.10.99
 - 139.28.37.250
 - SmartConsole query:
 - (src:151.241.99.207 OR dst:151.241.99.207 OR src:151.241.99.233 OR dst:151.241.99.233 OR src:158.62.198.182 OR dst:158.62.198.182 OR src:192.142.10.99 OR dst:192.142.10.99 OR src:139.28.37.250 OR dst:139.28.37.250)
- In SmartConsole, go to Logs & Monitor / Logs & Events > Audit Logs View and search for the query "Authentication method: application token".

Mitigation:

- Follow the [Check Point Hardening Best Practices Guide](#).
- Limit Trusted Clients (GUI clients) to trusted IP addresses/subnets:
 - In SmartConsole, go to Manage & Settings > Permissions & Administrators > Trusted Clients.
 - Double-click the client you want to edit.
 - In the Trusted Client configuration window that opens, change the settings as needed and.
 - Make sure do not use "Any" as a Type.
 - Click OK.
- Protect Management access with Firewall, restrict access to trusted IP addresses, and verify that implied rules for control connections are enabled. This will create an implied rule that will prevent management access for non-authorized IP addresses.

Recommendations:

We recommend the following actions be taken:

- Apply appropriate updates, hot fixes or mitigations provided by Check Point to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
 - **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
 - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
 - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
 - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a

- quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
 - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
 - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
 - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
 - **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
 - **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic. (**M1037: Filter Network Traffic**)
 - **Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure:** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
 - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
 - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
 - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References

<https://www.bleepingcomputer.com/news/security/check-point-patches-smartconsole-zero-day-exploited-in-attacks/>
<https://support.checkpoint.com/results/sk/sk185169/>

CVE

CVE-2026-16232

