مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Check Point Authentication Bypass Vulnerability

Tracking #:432319327

Date:23-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Check Point has disclosed an actively exploited authentication bypass vulnerability affecting multiple versions of Security Management Server and Multi-Domain Security Management Server (MDS).

TECHNICAL DETAILS:

Check Point has disclosed a high-severity authentication bypass vulnerability, CVE-2026-16232, affecting multiple versions of Security Management Server and Multi-Domain Security Management Server (MDS). The vulnerability is actively being exploited in the wild.

A successful exploit allows an unauthenticated remote attacker to obtain an application login token and authenticate to SmartConsole with full administrator privileges, enabling modification of security policies and management configurations.

Successful exploitation requires that the Management Server is accessible from the Internet and that Trusted Clients (GUI clients) are not properly restricted.

Vulnerability Details:

CVE-2026-16232 – Authentication Bypass via SmartConsole Application Token

- **Severity:** High
- **Impact:** Unauthenticated authentication bypass leading to full administrative access.
- Allows attackers to obtain an **application login token** without authentication.
- Enables login to **SmartConsole** with **full administrator privileges**.
- Attackers can modify security policies, security configurations, and management settings.
- Exploitation requires:
  - Internet access to the Management Server.
  - Trusted Clients configured insecurely (for example, allowing **"Any"**).
- Check Point has confirmed **active exploitation** affecting a limited number of customers.

Affected Products

- Check Point Security Management Server
- Check Point Multi-Domain Security Management Server (MDS)

Affected Versions

- R77.30 (End of Support)
- R80 (End of Support)
- R80.10 (End of Support)
- R80.20 (End of Support)
- R80.30 (End of Support)
- R80.40 (End of Support)
- R81 (End of Support)
- R81.10 (End of Support)
- R81.20
- R82
- R82.10

Fixed Version

- R82.10 Jumbo Hotfix Accumulator Take 36 or later
- R82 Jumbo Hotfix Accumulator Take 118 or later
- R81.20 Jumbo Hotfix Accumulator Take 158A or later

Indicators of Compromise (IoCs)

Known Attacker IP Addresses

- 151.241.99.207
- 151.241.99.233
- 158.62.198.182
- 192.142.10.99
- 139.28.37.250

SmartConsole Log 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)

Audit Log Search

Search the Audit Logs for:
Authentication method: application token
Unexpected or unauthorized use of application token authentication should be investigated immediately.

RECOMMENDATIONS:

Immediate Actions:

- Immediately install the latest Check Point Jumbo Hotfix Accumulator
- Restrict management access using firewall rules to trusted administrator IP addresses.
- Ensure implied control connection rules are enabled to block unauthorized management access.
- Review SmartConsole logs and audit logs for the published attacker IP addresses and any suspicious application token authentication events.
- Immediately investigate any unauthorized administrator logins or unexpected security policy changes.
- Follow Check Point's Security Management hardening best practices for long-term protection.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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