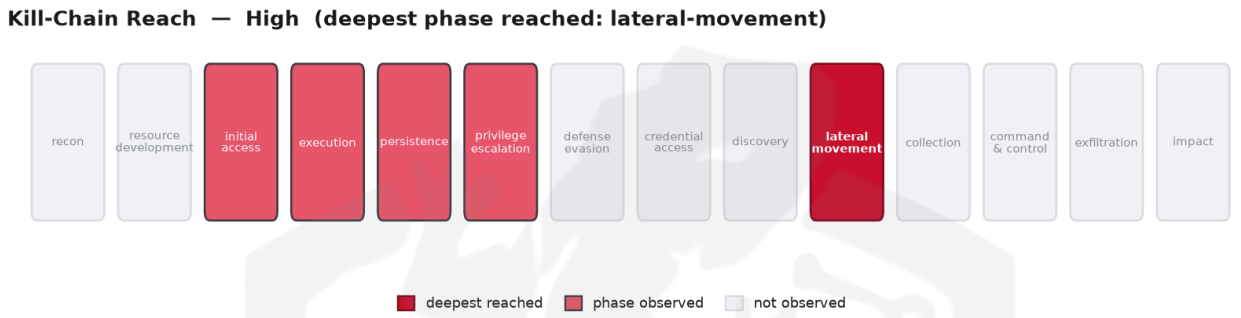
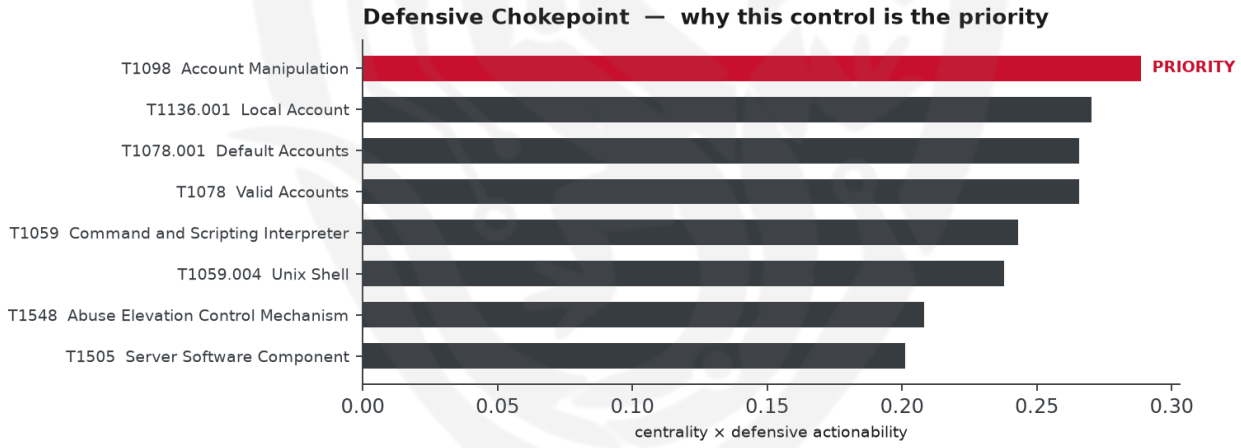
THREAT REPORT: EXPLOITATION OF CHECK POINT SMARTCONSOLE AUTHENTICATION BYPASS

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The observed cluster of activity involves the exploitation of CVE-2026-16232, a Check Point SmartConsole authentication bypass vulnerability, as well as other CVEs including CVE-2026-62145. The targeted systems and sectors are not specified due to insufficient data. Priority should be given to patching CVE-2026-62145 on all affected systems and monitoring for privilege and group changes. The threat actor behind this activity is not identified due to insufficient data.

Threat Overview

The threat actor, whose identity is not specified, is exploiting the Check Point SmartConsole authentication bypass vulnerability, specifically CVE-2026-16232 and CVE-2026-62145. The victimology and targeted

country are not available due to insufficient data. The malware families used in this campaign are also not specified.

Attack Chain and Priority Control

The observed techniques involve a chain of actions including creating or modifying system processes, impairing defenses, and exploiting public-facing applications. The priority technique is T1098 Account Manipulation, which is a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to Alert on privilege/group changes and credential additions to accounts (Event ID 4738/4670); review conditional-access changes. In parallel, patch CVE-2026-62145 on all affected systems.

Infrastructure and Corroboration

The malicious infrastructure is hosted on providers such as Ultahost Inc., Zemlyaniy Dmitro Leonidovich, and Shift Hosting LLC, as observed by third-party sources. According to abuse.ch, no malware families have been corroborated, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1543 Create or Modify System Process
- T1133 External Remote Services
- T1562 Impair Defenses
- T1190 Exploit Public-Facing Application
- T1550 Use Alternate Authentication Material
- T1562.004 Impair Defenses: Disable or Modify System Firewall
- T1078.001 Default Accounts
- T1136.001 Local Account
- T1548 Abuse Elevation Control Mechanism
- T1059 Command and Scripting Interpreter
- T1098 Account Manipulation
- T1059.004 Unix Shell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1068 Exploitation for Privilege Escalation
- T1505 Server Software Component
- T1543.002 Systemd Service
- T1136 Create Account
- T1484 Domain or Tenant Policy Modification
- T1550.001 Application Access Token

Analytical Scores

- Priority technique (graph chokepoint): T1098 Account Manipulation (centrality 0.3037).
- Operational risk: High (score 0.571, reaches lateral-movement).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.2801; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
FIN13	0.2801
HAFNIUM	0.2687
Scattered Spider	0.2662
APT5	0.262
GALLIUM	0.2531

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	139[.]28[.]37[.]250	AbuseIPDB 0% (UA) · AS47987 Zemlyaniy Dmitro Leonidovich
IP	151[.]241[.]99[.]207	AbuseIPDB 0% (US) · AS398256 Ultahost Inc.
IP	151[.]241[.]99[.]233	AbuseIPDB 0% (US) · AS398256 Ultahost Inc.
IP	158[.]62[.]198[.]182	AbuseIPDB 0% (US) · AS394177 Shift Hosting LLC

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1098 Account Manipulation (persistence)
- **Observed here:** T1098 Account Manipulation was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1547 Boot or Logon Autostart Execution (persistence)
- **Basis:** of the 12+ groups that use Account Manipulation, this pairing runs 2.0x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1547 Boot or Logon Autostart Execution in an attempt to maintain persistence, as this technique would allow them to execute malicious code automatically when a user logs on, potentially bypassing the blocked account manipulation control. This technique may be particularly appealing to the actor because it enables them to leverage existing user credentials to establish a foothold, rather than relying on compromised account credentials. The defensive countermeasure to mitigate this potential pivot would be to baseline and monitor autostart locations (Run keys, startup folders); alert on new persistence entries.

Also plausible (same tactic): T1542 Pre-OS Boot (n=3, lift 7.1), T1556 Modify Authentication Process (n=4, lift 4.7)

Detection and hardening for the pivot (T1547 Boot or Logon Autostart Execution)

- **Telemetry:** Sysmon (registry + process); EDR autostart/ASEP inventory
- **Detect:**
  - Sysmon 13 (registry value set) on Run/RunOnce keys under HKLM & HKCU ...\CurrentVersion\Run*
  - Sysmon 11 for shortcuts/scripts created in Startup folders
  - Periodic ASEP (autostart extensibility point) diff against a known-good baseline
- **Harden:**
  - Restrict write access to autostart registry keys and Startup folders
  - Application control to block unsigned autostart binaries
- **MITRE:** M1047 Audit, M1038 Execution Prevention · DS0019 Service, DS0024 Windows Registry, DS0022 File