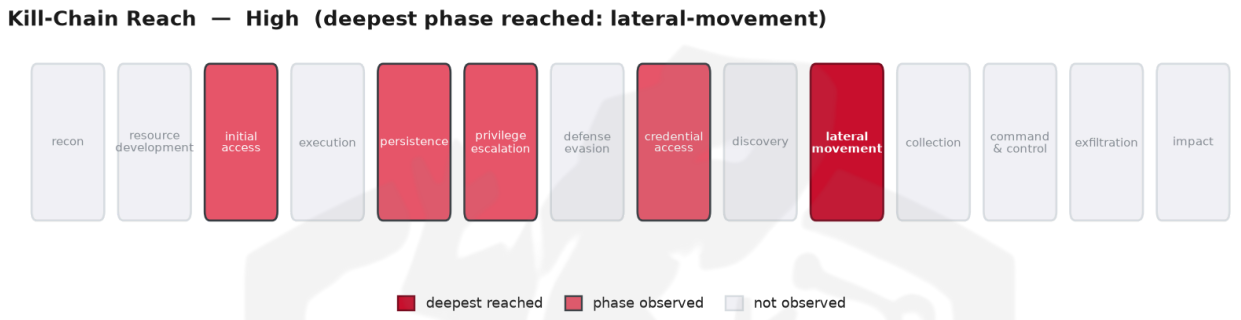
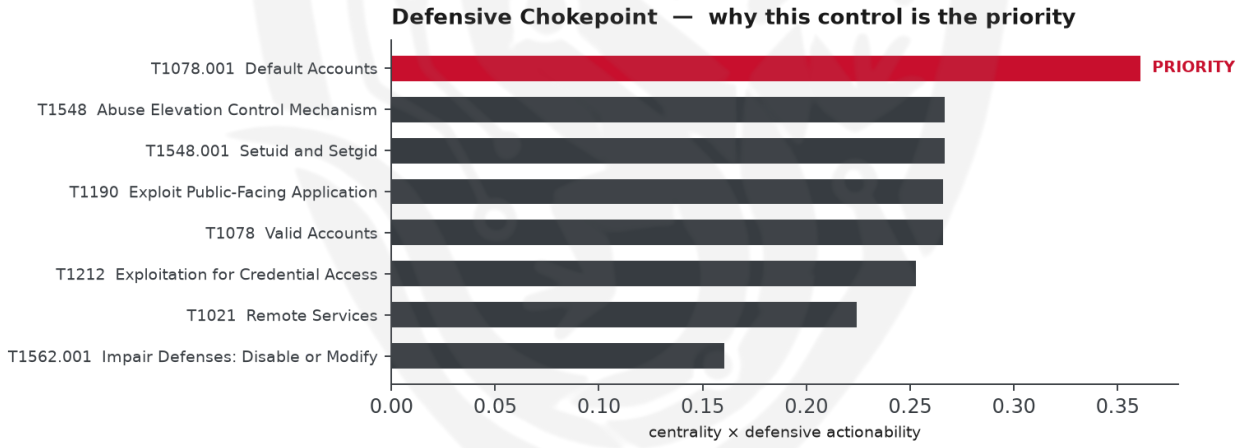
THREAT REPORT: CVE-2026-62144 EXPLOITATION CAMPAIGN

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 is exploiting the CVE-2026-62144 vulnerability, among others, to gain access to systems. The targeted country and sectors are not specified, but the threat actor is using various techniques to impair defenses and escalate privileges. Priority should be given to patching the CVE-2026-62144 vulnerability on all affected systems. The campaign's operational risk band is considered high, as it enables lateral movement.

Threat Overview

The threat actor, whose identity is not specified, is exploiting the CVE-2026-62144 vulnerability, as well as other vulnerabilities such as CVE-2026-16232 and CVE-2026-62145. The actor is using techniques such

as external remote services, impairing defenses, and exploiting public-facing applications to gain access to systems. The victimology of this campaign is not well understood due to insufficient data.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a chain that enables them to gain access to systems, impair defenses, and escalate privileges. The priority technique in this chain is T1078.001 Default Accounts, which is a key chokepoint. To mitigate this threat, the top priority control is to: Patch CVE-2026-62144 on all affected systems as the top priority, then: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted on providers such as Ultahost Inc., Zemlyaniy Dmitro Leonidovich, and Shift Hosting LLC. However, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, 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)

- T1133 External Remote Services
- T1562 Impair Defenses
- T1190 Exploit Public-Facing Application
- T1021 Remote Services
- T1078.001 Default Accounts
- T1548 Abuse Elevation Control Mechanism
- T1548.001 Setuid and Setgid
- T1212 Exploitation for Credential Access
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1068 Exploitation for Privilege Escalation
- T1021.001 Remote Desktop Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1078.001 Default Accounts (centrality 0.3611).
- Operational risk: High (score 0.571, reaches lateral-movement).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.294; 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
UNC3886	0.294
Axiom	0.2843
Akira	0.2722
Threat Group-1314	0.252
Agrius	0.2434

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:** T1078.001 Default Accounts (initial-access)

- **Observed here:** T1078.001 Default Accounts was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 29+ groups that use Default Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain their objective by leveraging WMI's native capabilities to execute commands and gather system information, potentially using it to scan for and exploit local vulnerabilities or to establish persistence. This technique may be particularly appealing as it allows the actor to blend in with legitimate system administration activities, making it harder to detect. To counter this potential move, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command