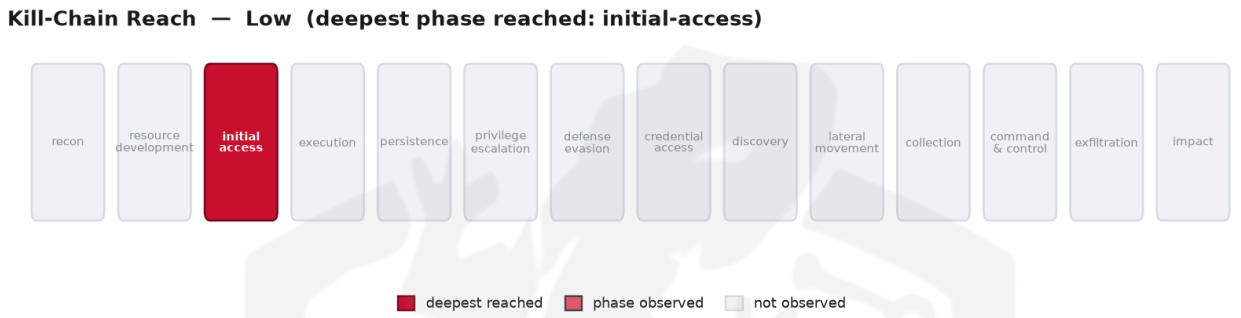
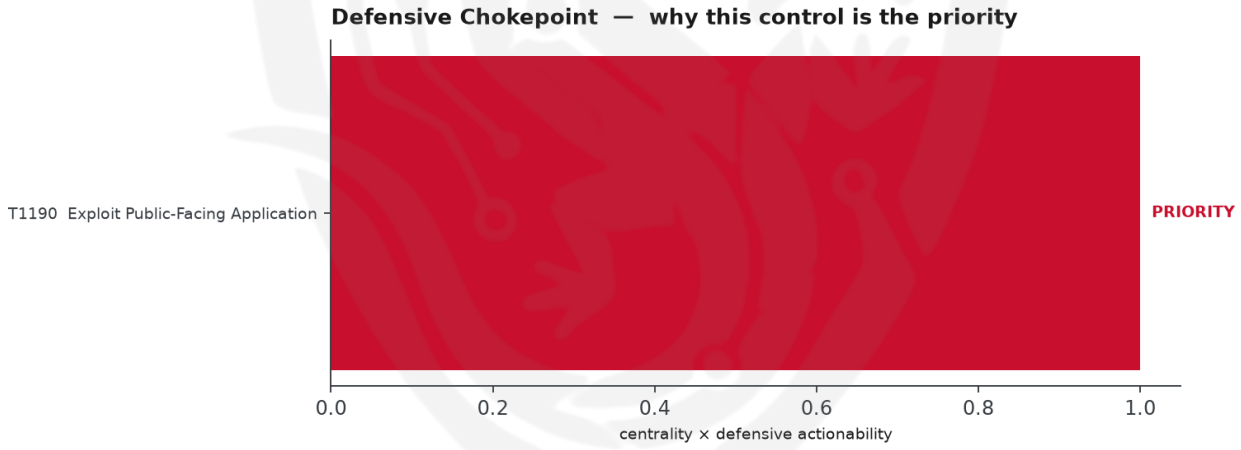
THREAT REPORT: EXPLOITATION OF PUBLIC-FACING APPLICATIONS VIA CVE-2026-39987

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 public-facing applications, specifically targeting CVE-2026-39987, among other vulnerabilities. The targeted country and sectors are not specified due to insufficient data. Priority should be given to patching the affected public-facing CVE immediately and applying a web application firewall (WAF) virtual patch. Additionally, restricting management interfaces to VPN-only and patching CVE-2026-39987 on all affected systems are crucial defensive actions.

Threat Overview

The threat actor, whose identity is not specified due to insufficient data, is exploiting public-facing applications using the CVE-2026-39987 vulnerability, along with several other CVEs. The techniques

inferred from the report include exploiting public-facing applications, which is the primary technique observed in this activity.

Attack Chain and Priority Control

The attack chain involves exploiting public-facing applications, with the priority technique being T1190 Exploit Public-Facing Application. The concrete control to mitigate this threat is to "Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only. In parallel, patch CVE-2026-39987 on all affected systems."

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence 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, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1190 Exploit Public-Facing Application

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 1.0).
- Operational risk: Low (score 0.117, reaches initial-access).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.378; 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
Volatile Cedar	0.378
GOLD SOUTHFIELD	0.2887
BlackTech	0.2236
Moses Staff	0.2236
BackdoorDiplomacy	0.2182

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

No indicators were attached to this pulse.

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:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** T1190 Exploit Public-Facing Application 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 22+ groups that use Exploit Public-Facing Application, this pairing runs 2.0x 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 access sensitive information, potentially using it to query system configurations or execute malicious code. This technique may be particularly appealing as it allows the actor to interact with the system in a way that blends in with legitimate administrative activity, making it harder to detect. To counter this, the mandated defensive control of monitoring wmiprvse.exe child-process creation, restricting remote WMI (DCOM) at the host firewall, and enabling WMI-Activity operational logging should be implemented.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=23, lift 1.5), T1059 Command and Scripting Interpreter (n=38, lift 1.2)

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