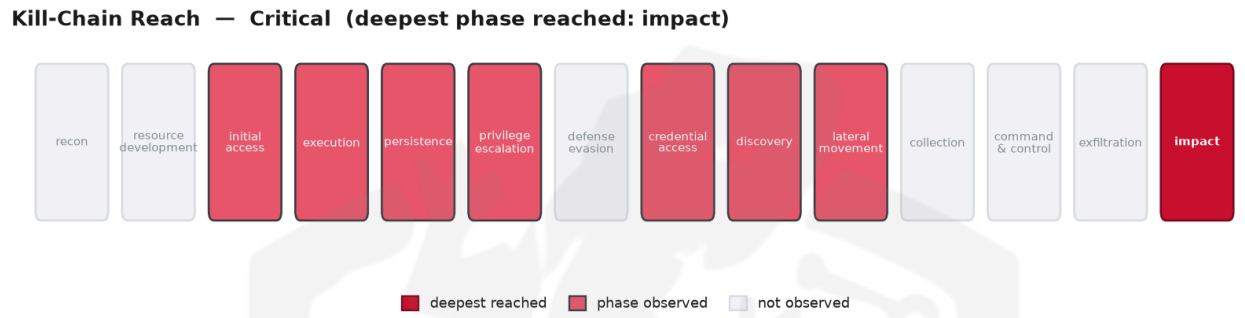
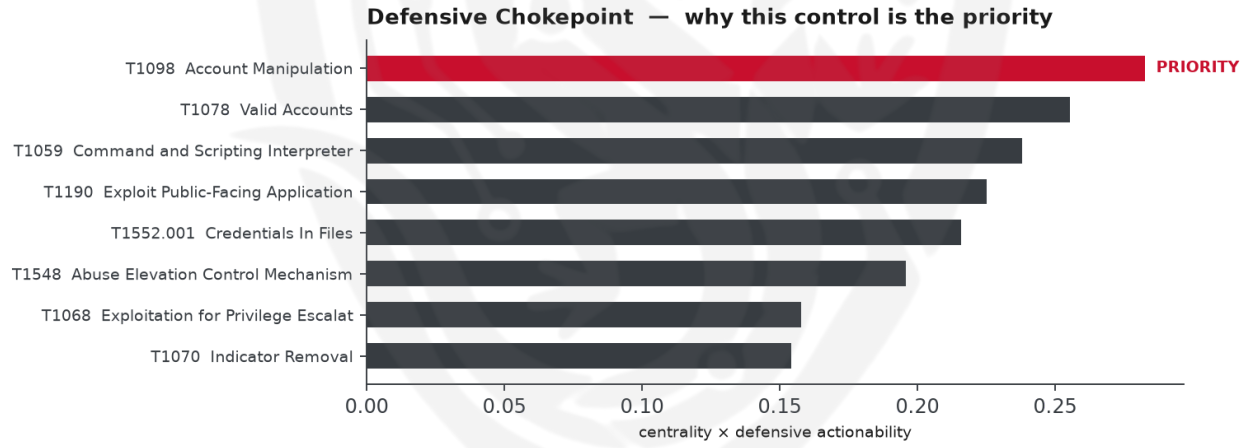
THREAT REPORT: UNKNOWN_ADVERSARY EXPLOITATION OF CVE-2026-20245

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 a zero-day vulnerability, CVE-2026-20245, in Cisco Catalyst SD-WAN Manager, with the priority defensive action being to patch the vulnerability on all affected systems. The threat actor is unknown, and the targeted country and sectors are insufficient to determine. Priority should be given to patching and monitoring for privilege and credential changes.

Threat Overview

The threat actor, whose identity is unknown, is exploiting the CVE-2026-20245 vulnerability in Cisco Catalyst SD-WAN Manager. The techniques used include external remote services, system information discovery, and exploit public-facing application, among others. The victimology is not well-defined due to insufficient data.

Attack Chain and Priority Control

The observed techniques form a chain that includes external remote services, system information discovery, and exploitation of public-facing applications, ultimately leading to account manipulation. The priority technique is T1098 Account Manipulation, which is the graph chokepoint. The priority control is to: Patch CVE-2026-20245 on all affected systems as the top priority, then: Alert on privilege/group changes and credential additions to accounts (Event ID 4738/4670); review conditional-access changes.

Infrastructure and Corroboration

The malicious infrastructure is hosted on various providers, including The Constant Company LLC, SoftBank Corp., NTT Docomo Business Inc., and Smart City Networks Limited Partnership. According to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. Abuse.ch has not corroborated any malware families in this campaign.

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
- T1087.001 Local Account
- T1021.004 SSH
- T1082 System Information Discovery
- T1190 Exploit Public-Facing Application
- T1070.006 Timestomp
- T1548 Abuse Elevation Control Mechanism
- T1059 Command and Scripting Interpreter
- T1070 Indicator Removal
- T1049 System Network Connections Discovery
- T1552.001 Credentials In Files
- T1098 Account Manipulation
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1068 Exploitation for Privilege Escalation
- T1003.008 /etc/passwd and /etc/shadow
- T1485 Data Destruction
- T1070.004 File Deletion
- T1136 Create Account

Analytical Scores

- Priority technique (graph chokepoint): T1098 Account Manipulation (centrality 0.2974).

- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4041; 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
APT5	0.4041
APT3	0.3678
FIN13	0.3528
Scattered Spider	0.3353
Play	0.332

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	126[.]51[.]108[.]152	AbuseIPDB 0% (JP) · AS17676 SoftBank Corp.
IP	153[.]186[.]231[.]233	AbuseIPDB 0% (JP) · AS4713 NTT Docomo Business Inc.
IP	167[.]179[.]79[.]189	AbuseIPDB 0% (JP) · AS20473 The Constant Company LLC
IP	207[.]190[.]37[.]94	AbuseIPDB 0% (US) · AS22827 Smart City Networks Limited Partnership
IP	209[.]137[.]225[.]101	AbuseIPDB 0% (US) · AS21947 Blackfoot Telephone Cooperative Inc.
IP	23[.]245[.]7[.]178	AbuseIPDB 0% (US) · AS11776 Breezeline

Type	Indicator	Context
IP	45[.]32[.]38[.]160	AbuseIPDB 0% (JP) · AS20473 The Constant Company LLC
IP	76[.]92[.]245[.]217	AbuseIPDB 0% (US) · AS11427 Charter Communications Inc
Hash	b82936f37648518425c7d3cf9e09eaffa41d7cdb3840f6a40287e3a108880f7b	

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