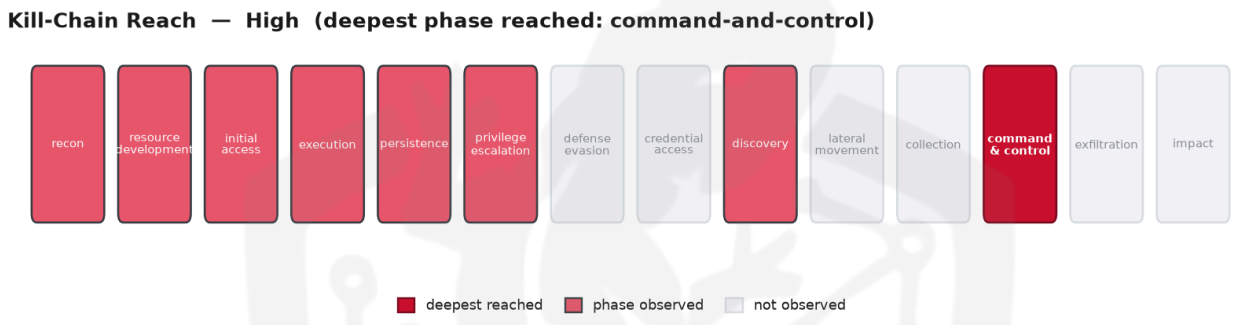
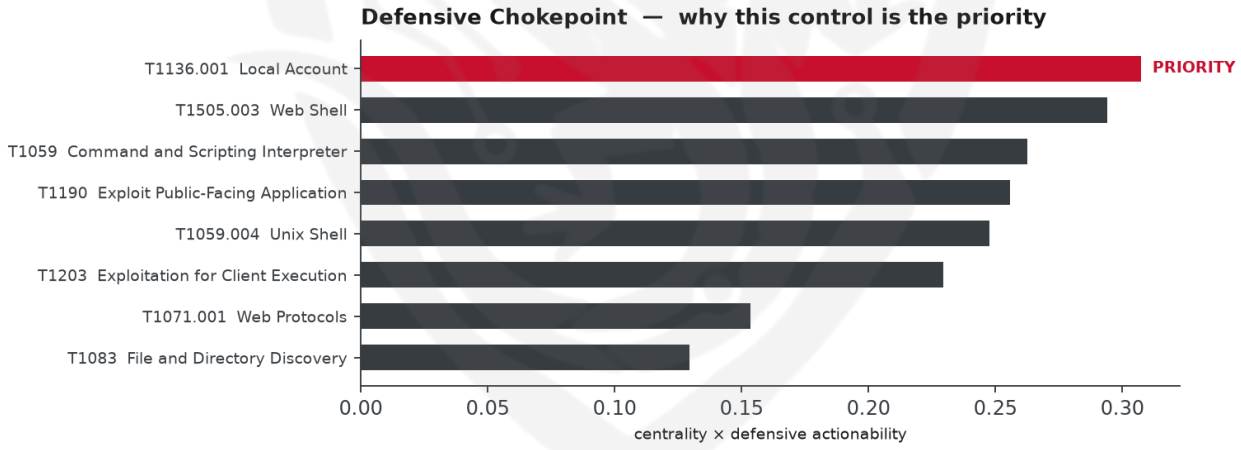
THREAT REPORT: UNAUTHENTICATED REMOTE CODE EXECUTION IN WORDPRESS CORE VIA CVE-2026-60137

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 vulnerability in WordPress Core, specifically CVE-2026-60137, to achieve unauthenticated remote code execution and full site takeover. The targeted systems are likely to be WordPress-based websites. Priority should be given to patching the vulnerability and monitoring for suspicious account activity. The threat actor's identity and motivations are currently unknown.

Threat Overview

The threat actor is exploiting the CVE-2026-60137 vulnerability in WordPress Core to gain control over targeted systems. The malware families used in this campaign are currently unknown. The victimology of

this threat is also unclear, with no specific country or sector being targeted.

Attack Chain and Priority Control

The attack chain involves exploiting the CVE-2026-60137 vulnerability, followed by techniques such as system information discovery, deobfuscation, and exploitation of public-facing applications. The priority technique is T1136.001 Local Account, which is a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to "Alert on new local/domain account creation (Event ID 4720/4728); enforce approval workflow for account provisioning. In parallel, patch CVE-2026-60137 on all affected systems."

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this threat. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with a confidence level of 80% or higher on AbuseIPDB.

Technical Appendix

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

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

- T1587.001 Malware
- T1588.006 Vulnerabilities
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1595.002 Vulnerability Scanning
- T1505.003 Web Shell
- T1136.001 Local Account
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1059.004 Unix Shell
- T1203 Exploitation for Client Execution
- T1071.001 Web Protocols
- T1046 Network Service Discovery
- T1105 Ingress Tool Transfer
- T1569.002 Service Execution
- T1078.003 Local Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1136.001 Local Account (centrality 0.3139).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4536; 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	0.4536
FIN13	0.3926
APT39	0.3771
TeamTNT	0.3695
Moses Staff	0.3578

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
Hash	12de8ce21bc534a968c327c00f2aa933b9034bc39b367ad1659f5aaa8be07744
Hash	37d86716edcb5b481d5d34b38b3bb4b522fcabdf0baf9b0523a0a61957620fad
Hash	4f4dc354dfa3ab9df33107b02106424d9940119363ceaff3399aefa8b14859dc
Hash	5588eb0d473bbc104ecb7d41037a747280eba03956a3d4c11368e4f0bd427ead
Hash	67ce5c125611078c2a6294faacd378b7dccbfb490641a0ca0822b071a22f759c
Hash	9c1bf6681ca94ab703d4f393fbfdd0acfb081285cd47ea4cf718ff9b71835722
Hash	d3e34d9306106aca15b1deb6dcfbe169c5f0df470bd22095845d553a60cbfd1e
Hash	d4cf7b5d8722236de52e9bad855b4ed4d99f18a561d192aec33525ec89557a7c
Hash	d8dfdab3a4358dbcd0eb129494d9e64b8392ef564bdc4cbe73e238c6d3ba51cd

Type	Indicator
Hash	ee8395666b9367967749757da27784922fdc18dc3e85db864d30fa703eb9db18

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:** T1136.001 Local Account (persistence)
- **Observed here:** T1136.001 Local Account was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1098 Account Manipulation (persistence)
- **Basis:** of the 13+ groups that use Local Account, this pairing runs 5.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1098 Account Manipulation to maintain access and evade detection by modifying existing account properties, such as adding a user to a privileged group, which would likely allow them to retain or escalate privileges despite the block on local account creation. This technique may be particularly appealing as it enables the actor to blend in with normal administrative activities, making it harder to detect. The defensive countermeasure to mitigate this potential pivot is to alert on privilege/group changes and credential additions to accounts (Event ID 4738/4670); review conditional-access changes.

Also plausible (same tactic): T1133 External Remote Services (n=10, lift 2.8), T1197 BITS Jobs (n=3, lift 4.6)

Detection and hardening for the pivot (T1098 Account Manipulation)

- **Telemetry:** Windows Security (account management); Azure AD audit logs
- **Detect:**
  - Security 4728/4732/4756 (added to security-enabled groups), 4738 (account changed), 4670 (permissions changed)
  - New credentials/keys added to accounts or app registrations in the IdP
  - MFA method added or reset outside a normal workflow
- **Harden:**
  - Alert on privileged-group changes; approval workflow for role grants
  - Monitor and restrict service-principal credential additions
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1018 User Account Management · DS0002 User Account, DS0026 Active Directory