INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-09 06:26 UTC

CashDro 3 Web Administration Panel Privilege Escalation via Authorization Bypass (CVE-2026-8077)

CVE VULNERABILITY | **HIGH** | CVSS 8.8

SCC Item ID	SCC-CVE-2026-0148
Type	CVE Vulnerability
CVE ID	CVE-2026-8077
Severity	HIGH
CVSS Base Score	8.8
Affected Products	CashDro 3 web administration panel, version 24.01.00.26
Published	2026-05-08
Discovery Source	Gemini

Executive Summary

A privilege escalation vulnerability in the CashDro 3 web administration panel allows an unauthenticated or low-privileged attacker to gain full administrative control of the system by manipulating a client-side permissions value. CashDro 3 version 24.01.00.26 is confirmed affected. Organizations running this point-of-sale management interface face complete administrative compromise if the panel is accessible over a network.

Technical Analysis

CVE-2026-8077 is a missing authorization vulnerability (CWE-862) in the CashDro 3 web administration panel, version 24.01.00.26. The root cause is server-side failure to enforce authorization checks; the application accepts or trusts a 'Permissions' field from the client and uses it to make authorization decisions without validating against server-stored role data, enabling privilege escalation to full administrative access without valid credentials or elevated session context. This pattern is consistent with CWE-285 (Improper Authorization) and CWE-639 (Authorization Bypass Through User-Controlled Key). MITRE ATT&CK mappings include T1548 (Abuse Elevation Control Mechanism) and T1565.002 (Stored Data Manipulation). A qualitative severity rating of High has been assigned; a CVSS base score of 8.8 is indexed by third-party aggregators (Tenable, Feedly, offseq) but has not been confirmed by NVD or the vendor. CVSS scoring by NVD is pending. EPSS data is not yet available. No CISA KEV listing. No vendor patch advisory has been identified from the available sources. Discovery and analysis informed by AI-assisted research.

Action Checklist

1. Step 1: Containment, Identify all instances of CashDro 3 version 24.01.00.26 in your environment. Immediately restrict network access to the web administration panel; block external access at the firewall or perimeter and limit access to trusted management networks or VPN-only segments. If the panel is internet-facing, take it offline until patched or mitigated.
2. Step 2: Detection, Review web server access logs on the CashDro 3 administration panel for anomalous requests that include modified or injected 'Permissions' fields in JSON payloads, unexpected privilege escalation events, or administrative actions from low-privileged or unauthenticated session tokens. Look for POST or PUT requests to admin endpoints from accounts not expected to hold administrative roles. No confirmed public IOCs are available at this time.
3. Step 3: Eradication, Contact the CashDro vendor directly for a patch or updated version that enforces server-side authorization checks. No vendor advisory or patch ID has been publicly confirmed as of 2026-03-04. Note: Direct vendor contact may not yield immediate remediation; establish a timeline expectation during initial contact and escalate if no patch is provided within 14 days. As an interim mitigation only: apply WAF rules to block or strip unexpected permission field modifications in JSON responses. This is not a substitute for server-side authorization enforcement; it is a temporary containment measure until the vendor patch is applied.
4. Step 4: Recovery, After applying vendor remediation, audit all administrative accounts created or modified on the CashDro 3 panel during the exposure window. Reset credentials for all administrative accounts, review audit logs for unauthorized configuration changes, and verify the panel enforces server-side authorization before returning it to production. Monitor admin panel activity for 30 days post-remediation.
5. Step 5: Post-Incident, This vulnerability exposes a systemic gap: reliance on client-controlled values for authorization decisions. Conduct a broader review of web application components, especially those handling role or permission data, to confirm server-side enforcement is in place. Consider adding this class of vulnerability (CWE-862, CWE-639) to your internal application security testing checklist and require vendor security attestations for POS and administration panel software in future procurement.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership and legal/compliance immediately if forensic review of CashDro 3 access logs identifies unauthorized administrative actions during the exposure window — particularly account creation, configuration changes, or access to payment or cardholder data — which may trigger PCI DSS breach notification obligations or applicable state/national data breach reporting requirements.

Recovery Notes	After applying vendor remediation, validate server-side authorization enforcement by replaying a crafted HTTP request with a manipulated 'Permissions' field to a CashDro admin endpoint and confirming a 403 response before returning the panel to production. Audit the full CashDro user account table against your pre-incident baseline to identify and remove any attacker-created administrative accounts, and review all POS configuration changes logged during the exposure window for signs of tampering. Maintain elevated log review cadence on the CashDro admin panel for 30 days post-remediation, specifically monitoring for POST/PUT requests to admin endpoints from non-administrative session contexts.
Forensic Artifacts	Web server access logs (Apache/Nginx access.log or IIS W3C logs) on the CashDro 3 panel host — filter for POST/PUT requests to admin-tier URI paths returning HTTP 200 from sessions authenticated with non-administrative roles, which is the direct signature of a successful CVE-2026-8077 authorization bypass. | CashDro 3 application-level audit log (internal to the platform, typically in /var/log/cashdro/ or equivalent) — review for admin-tier events (user creation, role assignment, configuration modification) attributed to accounts that should not hold administrative privileges, indicating successful privilege escalation via the client-side permissions manipulation. | HTTP request body captures (from WAF logs, ModSecurity audit log, or a network PCAP taken at the panel interface) — specifically look for JSON payloads containing a 'Permissions' field with a value inconsistent with the session's authenticated role tier, which is the mechanism of exploitation for this vulnerability. | CashDro 3 database user and role table export — a point-in-time snapshot capturing all accounts, role assignments, and creation/modification timestamps, used to identify net-new administrative accounts or unauthorized role escalations created during the exposure window. | Network flow or firewall session logs for the CashDro 3 panel port — identify any source IPs outside of trusted management network ranges that established sessions to the admin panel during the exposure window, providing attacker infrastructure attribution and confirming whether exploitation originated internally or externally.

Per-Action IR Details

Step 1: Containment — Identify all instances of CashDro 3 version 24.01.00.26 in your environment. Immediately restrict network access to the web administration panel; block external access at the firewall or perimeter and limit access to trusted management networks or VPN-only segments. If the panel is internet-facing, take it offline until patched or mitigated.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run 'nmap -p 80,443,8080,8443 --open ' or 'netstat -tlnp | grep ' on each segment to enumerate CashDro 3 panel instances. Apply an immediate iptables rule on the host: 'iptables -I INPUT -p tcp --dport -s -j ACCEPT && iptables -I INPUT -p tcp --dport -j DROP'. For perimeter routers without GUI, push an ACL denying any-to-panel-port from untrusted networks via CLI. A 2-person team can complete host-level firewall lockdown in under 30 minutes per site.

Evidence: Before isolating any CashDro 3 instance, capture a full snapshot of the web server access log (default path varies by deployment — check /var/log/cashdro/, /opt/cashdro/logs/, or IIS logs at C:\inetpub\logs\LogFiles\) to preserve pre-containment request history. Also capture a live netstat output ('netstat -antp | grep ') to document active sessions at time of containment, and dump current active session tokens from the CashDro session store or in-memory cache if accessible, to identify any sessions that may have already exploited the bypass.

Step 2: Detection — Review web server access logs on the CashDro 3 administration panel for anomalous requests that include modified or injected 'Permissions' fields in JSON payloads, unexpected privilege escalation events, or administrative actions from low-privileged or unauthenticated session tokens. Look for POST or PUT requests to admin endpoints from accounts not expected to hold administrative roles. No confirmed public IOCs are available at this time.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Use 'grep' or PowerShell to parse web server access logs for the specific exploit signature — search for POST or PUT requests containing the string 'Permissions' or 'permissions' in the request body alongside HTTP 200 responses to admin-tier endpoints: 'grep -E "(POST|PUT).*/admin" access.log | grep -i "permission"'. If logs include JSON body content, additionally filter for payloads where a permissions field value is inconsistent with the authenticated user's role tier. Deploy a ModSecurity WAF rule (free, open-source) on the CashDro host to inspect and log JSON request bodies for unexpected 'Permissions' key-value pairs in requests to admin routes, and alert on any match from a session authenticated as a non-admin role.

Evidence: Collect: (1) Web server access logs covering the full exposure window — filter for POST/PUT to any URI containing '/admin', '/manage', '/config', or equivalent CashDro admin endpoint paths, particularly those returning HTTP 200 or 302 from sessions authenticated with low-privilege or guest tokens. (2) Application-level audit logs within CashDro itself (if the platform maintains an audit trail) for admin-tier actions (user creation, permission changes, config modifications) attributed to non-administrative accounts. (3) Network capture (tcpdump or Wireshark on the panel interface) of any live or recent HTTP/HTTPS sessions to identify JSON payloads with a manipulated 'Permissions' field — specifically look for a field value inconsistent with the session's original authentication role.

Step 3: Eradication — Contact the CashDro vendor directly for a patch or updated version that enforces server-side authorization checks. No vendor advisory or patch ID has been publicly confirmed as of the configuration date. Do not rely on client-side permission fields for access control decisions as a workaround — apply WAF rules to block or strip unexpected permission field modifications in JSON responses if a vendor fix is not yet available.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-10 (Information Input Validation), NIST CM-7 (Least Functionality), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Until vendor patch is available, deploy a ModSecurity rule (CRS rule set, free) on the reverse proxy or web server fronting the CashDro 3 panel to intercept any HTTP request body containing a JSON key named 'Permissions' (case-insensitive) on admin-bound routes, and return HTTP 403 or strip the field before forwarding. Example ModSecurity rule pattern: 'SecRule REQUEST_BODY "@rx (?i)\"permissions\"\s*:\s*" "id:9001,phase:2,deny,status:403,log,msg:'CashDro CVE-2026-8077 Permissions field injection blocked'"'. Document all WAF rules as temporary compensating controls per your change management process and set a 30-day review trigger tied to vendor patch availability.

Evidence: Before applying any patch or WAF rule, preserve: (1) A file integrity hash (SHA-256 via 'sha256sum' or 'Get-FileHash') of all CashDro 3 application binaries and configuration files at version 24.01.00.26 — this establishes the pre-patch baseline and confirms no prior tampering. (2) A full export of the CashDro database user/role table to document the state of all accounts and privilege assignments before eradication, so any attacker-created admin accounts are captured. (3) The current server-side session store or token registry to identify sessions that may have operated with escalated privileges during the exposure window.

Step 4: Recovery — After applying vendor remediation, audit all administrative accounts created or modified on the CashDro 3 panel during the exposure window. Reset credentials for all administrative accounts, review audit logs for unauthorized configuration changes, and verify the panel enforces server-side authorization before returning it to production. Monitor admin panel activity for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), NIST SI-6 (Security and Privacy Function Verification), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Query the CashDro 3 user database directly to enumerate all accounts with admin-tier roles: 'SELECT username, role, created_at, last_login FROM users WHERE role = "admin" ORDER BY created_at DESC;' — flag any admin accounts created or role-elevated during the exposure window. For the 30-day post-remediation monitoring period without a SIEM, configure a cron job (Linux) or scheduled task (Windows) to run nightly log parsing: 'grep -E "(POST|PUT).*/admin" access.log >> /var/log/cashdro_admin_audit.log' and email the output to the IR team. Optionally deploy osquery with a query against the CashDro process and network socket table to alert on unexpected outbound connections from the panel service.

Evidence: Before returning the panel to production, capture: (1) A diff of the CashDro user/role table between pre-incident baseline export (from Step 3) and current state — any net-new admin accounts or role changes not attributable to authorized IT actions are attacker artifacts. (2) CashDro application audit log entries covering the full exposure window for configuration changes, user creation events, and payment or POS configuration modifications that may indicate attacker persistence or data access. (3) A test-verified HTTP response confirming that a crafted request with a manipulated 'Permissions' field to an admin endpoint now returns HTTP 403 or equivalent denial after patching — document this as proof-of-fix.

Step 5: Post-Incident — This vulnerability exposes a systemic gap: reliance on client-controlled values for authorization decisions. Conduct a broader review of web application components — especially those handling role or permission data — to confirm server-side enforcement is in place. Consider adding this class of vulnerability (CWE-862, CWE-639) to your internal application security testing checklist and require vendor security attestations for POS and administration panel software in future procurement.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SA-11 (Developer Testing and Evaluation), NIST SI-10 (Information Input Validation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Conduct a manual authorization bypass review of all other web-facing management panels in the environment (POS admin interfaces, inventory management, payment portals) by intercepting requests with OWASP ZAP (free) and manually testing whether submitting a modified role or permissions value in JSON or form POST bodies results in elevated access. Create a YARA rule or Sigma rule targeting HTTP log sources to detect future CWE-862/CWE-639 exploitation patterns (POST to admin endpoints with mismatched session privilege levels) and deploy it via log-grep automation or any open-source SIEM such as Wazuh. Add vendor security questionnaire requirements for server-side authorization validation to your procurement checklist.

Evidence: Preserve the full incident record — access logs, account audit exports, WAF rule change logs, and patch verification tests — for a minimum of 12 months per NIST AU-11 (Audit Record Retention) to support after-the-fact investigation, regulatory inquiry, or PCI DSS audit requirements given the POS nature of CashDro. Document the lessons-learned report referencing CWE-862 (Missing Authorization) and CWE-639 (Authorization Bypass Through User-Controlled Key) as the root cause classification to feed into future application security testing criteria.

Detection Guidance

Monitor web server access logs on the CashDro 3 administration panel for HTTP requests containing modified 'Permissions' field values in JSON payloads, particularly from sessions holding low-privileged or unauthenticated tokens. Flag any administrative actions, account creation, configuration changes, privilege assignments, performed by accounts not previously associated with administrative roles. Look for repeated or sequential requests to admin endpoints with varying permission field values, which may indicate enumeration or fuzzing activity. No confirmed public IOCs (IPs, hashes, signatures) are available for this CVE at this time. SIEM rules should alert on privilege escalation events within the application layer, not only at the OS or network level. Third-party indexing at Tenable and Feedly confirms the CVE is being tracked, but no public exploit code has been confirmed in available sources.

Framework Mappings

MITRE-ATTACK

- **T1548** — Abuse Elevation Control Mechanism
- **T1565.002** — Transmitted Data Manipulation

NIST-800-53R5

- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **AC-3** — Access Enforcement
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1565.002	Transmitted Data Manipulation	Impact

Sources

Source	URL	Tier
CVE-2026-8077 | Tenable®	https://www.tenable.com/cve/CVE-2026-8077	T3
CVE-2026-8077 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-8077	T3
CVE-2026-8077: CWE-862: Missing Authorization in CashDro ...	https://radar.offseq.com/threat/cve-2026-8077-cwe-862-missing-autho...	T3
How Cloudflare responded to the “Copy Fail” Linux vulnerability	https://blog.cloudflare.com/copy-fail-linux-vulnerability-mitigation/	T3
CVE-2026-7780 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-7780	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-8077	T1

Generated 2026-05-09 06:26 UTC by TJS Security Command Center