INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-25 13:43 UTC

Cisco Patches Critical Unauthorized API Access Vulnerability in Secure Workload

CVE VULNERABILITY | **CRITICAL** | CVSS 10.0

SCC Item ID	SCC-CVE-2026-0221
Type	CVE Vulnerability
Severity	CRITICAL
CVSS Base Score	10.0
Affected Products	Cisco Secure Workload
Published	2026-05-25
Discovery Source	Gemini

Executive Summary

Cisco disclosed and patched a critical vulnerability in Secure Workload (formerly Tetration) that allows an unauthenticated remote attacker to execute unauthorized API operations against the platform. The flaw carries a CVSS score of 10.0, the highest possible rating, meaning no credentials or user interaction are required for exploitation. Organizations running Cisco Secure Workload on-premises should treat this as an emergency patching event, as a successful attack could give an adversary full control over workload segmentation policy, telemetry data, and connected infrastructure.

Technical Analysis

The vulnerability affects Cisco Secure Workload (formerly Tetration) and is tracked under Cisco advisory identifier cisco-sa-csw-pnbsa-g8WEnuy. The CVE ID assignment is pending publication by NVD; consult the Cisco advisory directly for the most current CVE assignment. The flaw is classified under CWE-284 (Improper Access Control) and CWE-306 (Missing Authentication for Critical Function), meaning the API endpoint(s) in question can be invoked without any authentication challenge. CVSS base score is 10.0 (critical) per the Cisco advisory and NVD; the CVSS vector is pending publication and will be updated when NVD issues the official score. The attack vector is network-based, requires no privileges, and requires no user interaction, aligning with MITRE ATT&CK techniques T1078 (Valid Accounts, abuse of legitimate API access pathways) and T1190 (Exploit Public-Facing Application). Cisco has published a patch. As of this publication, CISA has not listed this vulnerability in the Known Exploited Vulnerabilities catalog; this is typical for newly disclosed vulnerabilities and does not indicate lower severity. Consult the Cisco advisory and NVD for current CVSS vector and EPSS data.

Action Checklist

1. Step 1: Containment. Immediately restrict network access to the Cisco Secure Workload management API and UI to documented administrative IP ranges via firewall rules. If the management interface is internet-facing, take it offline or place it behind a VPN with MFA until the patch is applied. This is a temporary measure; proceed immediately to Step 3 (patching).
2. Step 2: Detection. Query API gateway and application logs for unauthenticated or anomalous requests to Secure Workload API endpoints, particularly requests that received HTTP 200 responses with no session token or prior login event. Look for unexpected policy changes, new account creation, or configuration exports in Secure Workload audit logs. Monitor for T1190 indicators: high-frequency API calls from external IPs, calls to administrative endpoints from IPs outside your management subnet.
3. Step 3: Eradication. Apply the patch released by Cisco for Secure Workload as documented in advisory cisco-sa-csw-pnbsa-g8WEnuy. Identify the specific affected version(s) from the advisory and confirm your deployed version is covered. Follow Cisco's documented upgrade path for your deployment type (on-premises). Verify the patch closes the unauthenticated API access path by testing with an unauthenticated API call and confirming a 401 or 403 response.
4. Step 4: Recovery. After patching, validate that all Secure Workload API endpoints now require authentication. Review all Secure Workload audit logs for the exposure window for unauthorized policy changes, account additions, or data exports. Rotate any API keys or service account credentials associated with Secure Workload. Restore normal management access only after patch verification is complete.
5. Step 5: Post-Incident. Review how the Secure Workload management API was exposed and why unauthenticated access was possible. Audit all other management APIs in the environment for similar missing-authentication conditions (CWE-306 pattern). Implement firewall rules to ensure management interfaces are never internet-facing without authentication enforcement. Document the patching timeline and any exposure window for audit and regulatory purposes.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal counsel if Secure Workload audit log review reveals any unauthorized API calls during the exposure window that resulted in policy changes, account creation, or configuration exports — particularly if the platform enforces segmentation for environments containing PII, PHI, PCI-scoped workloads, or regulated data, as unauthorized access to a CVSS 10.0 unauthenticated API on a workload segmentation platform constitutes a presumptive breach requiring regulatory notification assessment.

Recovery Notes	After patching and credential rotation, maintain elevated monitoring of Secure Workload audit logs for a minimum of 30 days for any API activity from IP addresses identified in the exposure-window log review, as adversaries with prior unauthorized access may have implanted persistent API keys or service accounts that survived the rotation if the account inventory review was incomplete. Validate that all workload segmentation policies enforced by Secure Workload remain in their authorized state by comparing the post-recovery policy export against the last known-good configuration baseline. If no pre-incident baseline exists, treat the current policy set as unverified and schedule a manual policy review against your network segmentation design documentation before restoring full trust in the platform's enforcement posture.
Forensic Artifacts	Secure Workload API audit logs (exported via /openapi/v1/audit_logs or UI Platform > Audit Logs): primary evidence source for unauthenticated HTTP 200 responses on administrative endpoints, recording caller IP, endpoint path, HTTP method, response code, and session token presence — the direct artifact of CWE-306 exploitation on this platform. | Secure Workload user and API key inventory exports (/openapi/v1/users, /openapi/v1/roles, Platform > API Keys): forensic baseline for identifying accounts or keys created during the exposure window by an unauthenticated attacker who used the API access to establish persistence within the platform. | Secure Workload policy and scope configuration exports (/openapi/v1/policies, /openapi/v1/inventory_filters): evidence of attacker-induced segmentation policy tampering, which is the highest-impact action achievable via unauthorized API access to a workload segmentation platform and may have enabled lateral movement across enforced network segments. | Perimeter and host-based firewall connection logs for the Secure Workload management VIP on TCP 443: network-layer evidence establishing which external or internal source IPs reached the management API during the exposure window, used to scope the attacker IP set and determine if exploitation was opportunistic or targeted. | Secure Workload cluster application logs at /local/logs/ on cluster nodes: platform-level evidence of how the authentication bypass was processed by the API framework, which may reveal exploit payload characteristics (unusual HTTP headers, malformed tokens, specific endpoint sequences) useful for threat hunting across other management APIs in the environment for the same CWE-306 pattern.

Per-Action IR Details

Step 1: Containment — Immediately restrict network access to the Cisco Secure Workload management API and UI to known administrative IP ranges via perimeter ACLs or firewall rules. If the management interface is internet-facing, take it offline or place it behind a VPN with MFA enforced (NIST AC-17, CIS 6.4) until the patch is applied. Consult Cisco advisory cisco-sa-csw-pnbsa-g8WEnuy for any Cisco-recommended interim workarounds.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: On Linux-based Secure Workload infrastructure nodes, apply an immediate iptables or nftables rule restricting TCP 443 (API/UI port) to your documented admin IP list: `iptables -I INPUT -p tcp --dport 443 ! -s -j DROP`. On edge firewalls, implement an explicit deny-all inbound ACL to the Secure Workload cluster management VIP, permitting only enumerated admin source IPs. If VPN is not available, use SSH port-forwarding as a temporary authenticated tunnel for admin access. Document the ACL change with timestamp for the exposure window calculation.

Evidence: Before applying ACL changes, capture a full netstat or `ss -tnp` snapshot on the Secure Workload cluster nodes to record any active or recently established TCP sessions on the management API port (default 443). Export

firewall connection-state tables and any existing perimeter firewall logs showing inbound connections to the Secure Workload management VIP for the 30-day window preceding discovery — these establish the exposure window and identify source IPs that reached the unauthenticated API endpoint prior to containment.

Step 2: Detection — Query API gateway and application logs for unauthenticated or anomalous requests to Secure Workload API endpoints, particularly requests that bypassed authentication (HTTP 200 responses with no session token or prior login event). Look for unexpected policy changes, new account creation, or configuration exports in Secure Workload audit logs. Cross-reference against NIST AU-2 and AU-6 logging requirements. Monitor for T1190 indicators: high-frequency API calls from external IPs, calls to administrative endpoints from IPs outside your management subnet.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query Secure Workload's built-in audit log export (available under Platform > Audit Logs in the UI, or via the `/openapi/v1/audit_logs` API endpoint if still accessible from a trusted host) and pipe the JSON output through `jq` to filter for HTTP 200 responses lacking a preceding authentication event: `jq '.[] | select(.response_code == 200 and (.auth_method == null or .auth_method == ""))' audit_export.json`. Cross-reference source IPs against known admin ranges using a simple bash script with a whitelisted IP file. For network-layer detection, run a Wireshark or tcpdump capture on the management interface filtered for `tcp port 443 and not src net ` to identify any ongoing unauthorized access attempts after ACL containment.

Evidence: Export Secure Workload audit logs covering the full exposure window (from the last confirmed-clean state to containment time) — these logs record API caller IP, endpoint called, HTTP method, response code, and whether a valid session token was present. Specifically hunt for API calls to administrative endpoints such as `/openapi/v1/users`, `/openapi/v1/roles`, `/openapi/v1/policies`, and `/openapi/v1/inventory_filters` that returned HTTP 200 without a correlated authentication event. Capture any Secure Workload application-level logs from `/local/logs/` on cluster nodes for evidence of unauthenticated request handling by the API framework, which would indicate CVE exploitation rather than misconfiguration.

Step 3: Eradication — Apply the patch released by Cisco for Secure Workload as documented in advisory cisco-sa-csw-pnbsa-g8WEnuy. Identify the specific affected version(s) from the advisory and confirm your deployed version is covered. Follow Cisco's documented upgrade path for your deployment type (on-premises). Verify the patch closes the unauthenticated API access path by reviewing Cisco's fixed-version confirmation in the advisory (NIST SI-2, CIS 7.3, CIS 7.4).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For a 2-person team managing an on-premises Secure Workload deployment without automated patch orchestration, download the patch bundle directly from Cisco's Software Download portal using the exact build identifier in advisory cisco-sa-csw-pnbsa-g8WEnuy. Verify the SHA-512 checksum of the downloaded bundle against the value published in the advisory before staging: `sha512sum `. Follow Cisco's offline upgrade procedure for Secure Workload on-premises (documented in the Cisco Secure Workload Installation and Upgrade Guide for your hardware generation — M5, M6, or virtual appliance). Snapshot or checkpoint cluster state before applying if your hypervisor supports it.

Evidence: Before patching, preserve a complete copy of the Secure Workload cluster's current configuration state: export all tenant policies, user accounts, roles, and network scopes via the API (`/openapi/v1/policies`, `/openapi/v1/users`, `/openapi/v1/roles`) and store with a cryptographic hash for post-patch integrity comparison. Capture the current software version string from the Secure Workload UI (Platform > Upgrade) and record it in the incident timeline. These exports serve as the baseline to detect any unauthorized changes made during the exploitation window that must be reviewed or rolled back as part of eradication.

Step 4: Recovery — After patching, validate that all Secure Workload API endpoints now require authentication by testing with an unauthenticated request and confirming a 401 or 403 response. Review all Secure Workload audit logs for the exposure window for unauthorized policy changes, account additions, or data exports. Rotate any API keys or service account credentials associated with Secure Workload (NIST AC-2, D3-CRO). Restore normal management access only after patch verification is complete.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Validate the authentication fix with a simple curl test from an unauthenticated context: `curl -k -o /dev/null -w "%{http_code}" https:///openapi/v1/users` — a patched system must return 401 or 403, not 200. For credential rotation without a PAM tool, enumerate all Secure Workload API keys via the UI (Platform > API Keys) and invalidate all keys issued before the patch date; generate new keys with minimum required scopes per integration. For service accounts, cross-reference the Secure Workload user inventory export (captured pre-patch) against your authoritative directory to identify any accounts created during the exposure window that do not have a corresponding provisioning ticket.

Evidence: Diff the pre-patch and post-patch exports of Secure Workload user accounts, roles, and policy configurations (captured during Step 3 eradication) to identify any additions, modifications, or deletions that occurred during the exposure window. Pay particular attention to new user accounts with admin or owner roles, new API keys with broad scopes, and policy changes that broadened network access or disabled segmentation enforcement — these are the highest-value actions an attacker would perform via unauthorized API access to a workload segmentation platform. Preserve all audit log exports with chain-of-custody documentation before ACL rollback.

Step 5: Post-Incident — Review how the Secure Workload management API was exposed and why unauthenticated access was possible. Audit all other management APIs in the environment for similar missing-authentication conditions (CWE-306 pattern). Formalize network segmentation controls to ensure management interfaces are never internet-facing without authentication enforcement (NIST AC-3, AC-6, CIS 4.4). Implement API access monitoring as a standing detection rule referencing AU-6 and D3-UAP. Document the patching timeline and any exposure window for future audit and regulatory purposes.

NIST Phase: Post Incident

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy a standing Sigma rule targeting Secure Workload API logs for the CWE-306 exploitation pattern — specifically HTTP 200 responses on administrative API endpoints with absent or null authentication tokens — and schedule weekly log review against this rule if no SIEM is available. For the broader CWE-306 audit, use a lightweight port scanner (nmap with `-sV`) against your internal management network to enumerate all services on ports 443/8443/8080 and cross-reference discovered services against an expected-authentication matrix. Document findings in a risk register with remediation owners. Use `osquery` with the `listening_ports` and `process_open_sockets` tables on management hosts to maintain a standing inventory of exposed API services.

Evidence: Compile the complete incident timeline: first possible exposure date (earliest log evidence or deployment date of the vulnerable version), containment timestamp (ACL applied), patch application timestamp, and credential rotation completion timestamp. Preserve all audit log exports, configuration diffs, and network capture files in write-once storage with SHA-256 hashes for regulatory documentation. If unauthorized policy changes to Secure Workload segmentation rules were detected during recovery review, treat as a potential data-path integrity event and escalate to determine whether the segmentation changes facilitated lateral movement or data exfiltration during the exposure window.

Detection Guidance

Primary detection target: unauthenticated API requests against Cisco Secure Workload management endpoints. Review Secure Workload application and API access logs for requests that received successful responses (HTTP 200/201/202) without a corresponding authenticated session token or prior login event. Flag requests to administrative API paths originating from IPs outside your documented management subnet. Look for bulk or sequential API calls suggesting automated enumeration or policy manipulation. In your SIEM, correlate Secure Workload API logs with authentication logs: a successful API operation with no matching auth event is a high-confidence indicator of exploitation. Also review audit logs within Secure Workload for unexpected changes: new accounts, policy modifications, segment rule changes, or data exports occurring during the exposure window. MITRE T1190 behavioral indicators include high-rate external requests to the management interface; T1078 indicators include API sessions that do not trace back to a known user account. No public IOCs were available at time of writing.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Cisco Secure Workload Unauthorized API Access ...	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
View Vulnerability Dashboard [Cisco Secure Workload]	https://www.cisco.com/c/en/us/td/docs/security/workload_security/se...	T3
Cisco Secure Workload Datasheet	https://www.cisco.com/c/en/us/products/collateral/data-center-analy...	T3
Critical vulnerability in Cisco Secure Workload rated at ...	https://www.csoonline.com/article/4175913/critical-vulnerability-in...	T3
Cisco Issues Critical Patch for Secure Workload Vulnerability	https://www.reddit.com/r/pwnhub/comments/1tjn7s7/cisco_issues_criti...	T3

Generated 2026-05-25 13:43 UTC by TJS Security Command Center