INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-21 06:59 UTC

CVE-2026-20223: Cisco Secure Workload Zero-Auth REST API Flaw Enables Cross-Tenant Site Admin Access (CVSS 10.0)

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0204
Type	CVE Vulnerability
CVE ID	CVE-2026-20223
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Cisco Secure Workload (SaaS and on-premises): releases 3.9 and earlier (all versions), 3.10 prior to 3.10.8.3, 4.0 prior to 4.0.3.17
Published	2026-05-20T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Cisco disclosed a maximum-severity vulnerability in Cisco Secure Workload that allows any unauthenticated attacker on the network to access internal REST APIs with Site Administrator privileges and cross tenant boundaries. No credentials, user interaction, or special conditions are required. Organizations running on-premises deployments on versions 3.10 prior to 3.10.8.3, or 4.0 prior to 4.0.3.17, are fully exposed with no available workaround; SaaS deployments have been patched by Cisco without customer action.

Technical Analysis

CVE-2026-20223 is a missing authentication vulnerability (CWE-306, CWE-287, CWE-862) in Cisco Secure Workload's internal REST API layer. The flaw allows an unauthenticated remote attacker to invoke privileged API endpoints that should require Site Admin authentication, and to traverse tenant isolation boundaries in multi-tenant deployments. Attack vector is network, complexity is low, no privileges are required, and no user interaction is needed, consistent with a CVSS 9.5 critical rating. MITRE techniques applicable: T1190 (Exploit Public-Facing Application), T1078.004 (Valid Accounts: Cloud Accounts, applicable to tenant impersonation), T1548 (Abuse Elevation Control Mechanism). Affected versions: all releases 3.9 and earlier (no patch path available), 3.10 prior to 3.10.8.3, 4.0 prior to 4.0.3.17. Fixed releases: 3.10.8.3 and 4.0.3.17. Cisco SaaS deployments were patched server-side; on-premises operators must upgrade. No workaround exists. Note: A

CVSS score discrepancy exists between available source data (9.5) and some advisory language (10.0); analysts should verify against the official Cisco advisory and NVD record at https://nvd.nist.gov/vuln/detail/CVE-2026-20223 (verified as of 2026-03-04).

Action Checklist

1. Step 1: Containment. Immediately identify all on-premises Cisco Secure Workload deployments running versions 3.9 and earlier, 3.10 prior to 3.10.8.3, or 4.0 prior to 4.0.3.17. Restrict network access to the Secure Workload management plane and internal REST API endpoints at the perimeter firewall or upstream network controls. If running 3.9 or earlier with no patch path, escalate immediately to Cisco TAC for migration guidance and isolate the deployment from tenant workloads. Confirm SaaS deployments are already patched by reviewing Cisco's advisory. Reference: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection. Query API gateway and application logs on the Secure Workload cluster for unauthenticated REST API calls, particularly those invoking Site Admin-scoped endpoints or returning 200/201 responses without an associated authentication token. Look for cross-tenant API calls where the requesting tenant context does not match the resource tenant context. Review access logs for anomalous source IPs calling internal API paths. If Cisco Secure Workload audit logging is enabled, filter for privilege-level actions (Site Admin operations) with no corresponding login event. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs), D3-LAM (Local Account Monitoring), D3-SFA (System File Analysis).
3. Step 3: Eradication. For deployments on version 3.10, upgrade to 3.10.8.3. For deployments on version 4.0, upgrade to 4.0.3.17. Obtain packages from the Cisco Software Center using your entitlement. Deployments on version 3.9 or earlier have no listed patch path; contact Cisco TAC immediately for migration guidance. Do not leave unpatched deployments accessible on any network segment. Reference: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery. After patching, validate the upgrade version string in the Cisco Secure Workload console. Conduct a privilege audit of all Site Admin accounts to identify any unauthorized accounts or configuration changes introduced during the exposure window. Review tenant boundary configurations for unauthorized cross-tenant policy modifications. Restore API gateway logging to full verbosity and monitor for at least 72 hours post-patch for residual unauthorized API activity. Reference: NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), D3-CRO (Credential Rotation), D3-UAP (User Account Permissions).
5. Step 5: Post-Incident. Review your vulnerability management process to assess mean time to patch for critical Cisco advisories on infrastructure management software. Evaluate whether internal REST API endpoints for administrative platforms are adequately segmented from untrusted network zones. Implement network-layer controls to restrict management plane access to authorized management IP ranges only. Review CWE-306 (Missing Authentication for Critical Function) as a recurring control gap in your vendor assessment criteria. Reference: NIST AC-17 (Remote Access), NIST AC-6 (Least Privilege), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), D3-MFA (Multi-factor Authentication), D3-CH (Credential Hardening).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance immediately if API access logs show any HTTP 200/201 responses to Site Admin-scoped Secure Workload REST API endpoints from IPs outside the authorized management network range during the exposure window, as this indicates confirmed unauthorized access with cross-tenant Site Admin privilege and potential breach of workload policy data across all hosted tenants, triggering breach notification assessment under applicable data protection regulations.
Recovery Notes	After patching to 3.10.8.3 or 4.0.3.17, verify the fix is effective by attempting an unauthenticated REST API call against a Site Admin endpoint from a test client outside the management network — the patched version should return HTTP 401 or 403 with no data disclosure. Maintain full API access log verbosity for a minimum of 72 hours post-patch and retain those logs for at least 90 days to support any subsequent forensic or regulatory inquiry. Because CVE-2026-20223 permitted cross-tenant policy modification with no authentication, all tenant workload policies and scope definitions must be reviewed against known-good baselines before declaring the environment clean, regardless of whether active exploitation is confirmed.
Forensic Artifacts	Cisco Secure Workload REST API access logs (typically under /local/logs/ on the cluster nodes): look for HTTP GET/POST/PUT/DELETE requests to /openapi/v1/ paths — especially /users, /roles, /scopes, /policies — returning 200/201 with no Authorization header present, which is the direct signature of zero-auth exploitation of CVE-2026-20223 | Cisco Secure Workload audit log: filter for Site Admin-level operations (account creation, role assignment, scope modification, tenant boundary changes) with timestamps during the exposure window and no corresponding authenticated login event for the source IP — this distinguishes exploitation from legitimate admin activity | Perimeter firewall or network flow records (NetFlow/IPFIX or firewall session logs): source IPs and session counts targeting the Secure Workload cluster's management plane ports (443 and any additional internal API listener ports) from non-management IP ranges, particularly any IPs with high request volumes or scanning patterns across /openapi/ path space | Cisco Secure Workload configuration export (pre-patch): a JSON/XML dump of all tenant scopes, workload policies, and Site Admin account definitions captured before patching — diff against a known-good baseline to identify unauthorized accounts added, policies modified, or tenant boundary rules changed by an attacker leveraging cross-tenant Site Admin access | On-premises Secure Workload cluster system logs (syslog/journal): entries from the API service process showing authentication bypass events, internal authorization decisions returning elevated privilege grants without credential validation, or unexpected process behavior consistent with API abuse — relevant specifically for 3.9 and earlier deployments where full compromise must be assumed

Per-Action IR Details

Step 1: Containment — Immediately identify all on-premises Cisco Secure Workload deployments running versions 3.9 and earlier, 3.10 prior to 3.10.8.3, or 4.0 prior to 4.0.3.17. Restrict network access to the Secure Workload management plane and internal REST API endpoints at the perimeter firewall or upstream network controls. If running 3.9 or earlier with no patch path, treat the deployment as fully compromised and isolate it from tenant workloads pending vendor guidance. Confirm SaaS deployments are already patched by reviewing Cisco's advisory. Reference: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Use `iptables` or Windows Firewall (netsh advfirewall) to immediately block inbound TCP on Cisco Secure Workload REST API ports (default 443 and any internally exposed API listener ports — verify against your deployment's network map) from all sources except a designated management jump host. Run `ss -tlnp | grep ` (Linux) or `netstat -ano` (Windows) on the Secure Workload nodes to enumerate all active listeners before applying rules. Document the current `iptables -L -n -v` output as a baseline artifact before changes.

Evidence: Before restricting network access, capture: (1) full netflow or perimeter firewall session logs showing all source IPs that reached the Secure Workload management plane API ports within the past 30 days; (2) a snapshot of the Cisco Secure Workload cluster's active network listener state (`ss -tlnp` output) to confirm which API ports are exposed; (3) the current Secure Workload cluster version string from the admin console or via CLI (`rpm -qa | grep -i tetration` or equivalent) to document the exposure window definitively.

Step 2: Detection — Query API gateway and application logs on the Secure Workload cluster for unauthenticated REST API calls, particularly those invoking Site Admin-scoped endpoints or returning 200/201 responses without an associated authentication token. Look for cross-tenant API calls where the requesting tenant context does not match the resource tenant context. Review access logs for anomalous source IPs calling internal API paths. If Cisco Secure Workload audit logging is enabled, filter for privilege-level actions (Site Admin operations) with no corresponding login event. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs), D3-LAM (Local Account Monitoring), D3-SFA (System File Analysis).

NIST Phase: Detection Analysis

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

Controls: NIST AU-3 (Content of Audit Records), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, grep the Cisco Secure Workload application log directory (typically `/local/logs/` or the path defined in your deployment's syslog config) using: `grep -E 'HTTP/(1\.[01]|2) (200|201|204)' access.log | grep -v 'Authorization:'` to surface HTTP success responses with no auth header. Then cross-reference with: `grep -i 'site.admin\|root_scope\|cross.tenant' audit.log` to identify Site Admin-scoped operations. Use `awk '{print $1}' access.log | sort | uniq -c | sort -rn | head -20` to rank source IPs by request volume and flag any non-management-range IPs with high 200-series response counts.

Evidence: Before modifying or rotating logs, preserve: (1) the full Cisco Secure Workload REST API access log file (raw, unfiltered) covering the period from the vulnerability disclosure date back to the earliest retained log — this is the primary exploitation evidence source for CVE-2026-20223 because zero-auth exploitation leaves no authentication token in the request headers; (2) the Secure Workload audit log showing all Site Admin-level operations (account creation, policy modification, tenant scope changes) with timestamps; (3) a list of all API endpoints called with HTTP 200/201 responses from IPs outside the defined management network range — cross-tenant boundary crossings will appear as API calls to tenant-scoped resource paths with a source tenant context mismatch.

Step 3: Eradication — For deployments on version 3.10, upgrade to 3.10.8.3. For deployments on version 4.0, upgrade to 4.0.3.17. Obtain packages from the Cisco Software Center using your entitlement. Deployments on version 3.9 or earlier have no listed patch path; contact Cisco TAC immediately for migration guidance. Do not leave unpatched deployments accessible on any network segment. Reference: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).

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 7.1 (Establish and Maintain a Vulnerability Management

Process)

Compensating: Before applying the Cisco patch, take a full configuration export from the Secure Workload console (Manage → Configuration Export) and store it offline as a pre-patch baseline. After applying Cisco Secure Workload 3.10.8.3 or 4.0.3.17 from Cisco Software Center (software.cisco.com — verify the package SHA checksum against Cisco's published hash in the advisory before installation), verify the installed version via the cluster CLI: `tetration_installer --version` or by checking the About page in the Secure Workload console. For 3.9 and earlier deployments isolated in Step 1, open a Cisco TAC case with priority P1, referencing CVE-2026-20223 explicitly — do not reconnect these nodes to any network segment until TAC provides a migration path.

Evidence: Before patching, capture: (1) a full Cisco Secure Workload configuration export to document the state of all tenant policies, scope definitions, and Site Admin accounts at the time of eradication — any unauthorized accounts or policy modifications introduced via exploitation of CVE-2026-20223 will be visible by diffing this export against a known-good baseline; (2) the pre-patch version string and patch level from the cluster (for chain-of-custody documentation); (3) on-disk integrity of the Secure Workload application binaries if compromise of 3.9 or earlier is suspected — collect file hashes of the API service binaries before replacement.

Step 4: Recovery — After patching, validate the upgrade version string in the Cisco Secure Workload console. Conduct a privilege audit of all Site Admin accounts to identify any unauthorized accounts or configuration changes introduced during the exposure window. Review tenant boundary configurations for unauthorized cross-tenant policy modifications. Restore API gateway logging to full verbosity and monitor for at least 72 hours post-patch for residual unauthorized API activity. Reference: NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), D3-CRO (Credential Rotation), D3-UAP (User Account Permissions).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Run the Cisco Secure Workload API to enumerate all Site Admin accounts: `curl -sk -H 'Authorization: ' https:///openapi/v1/users?role=site_admin` and compare the output against your documented baseline of authorized Site Admin accounts. Diff the pre-patch configuration export (captured in Step 3) against a post-patch export using a JSON diff tool (`jq` + `diff`) to surface any tenant scope modifications, policy changes, or new scopes created during the exposure window. Monitor the Secure Workload access log in real time post-patch using `tail -f /local/logs/access.log | grep -E '(200|201)' ` watching for any repeat of the unauthenticated access pattern.

Evidence: During recovery validation, capture: (1) the post-patch Site Admin account list (full export via API) timestamped immediately after patching, to serve as the verified clean baseline for future audits; (2) a diff of pre- and post-patch tenant boundary policies to document whether any unauthorized cross-tenant scope changes persist after patching — CVE-2026-20223 allowed cross-tenant Site Admin access, meaning an attacker could have modified workload policies across tenant boundaries that survive the patch; (3) 72-hour post-patch API access logs to confirm no residual unauthorized activity from IPs identified as suspicious in Step 2.

Step 5: Post-Incident — Review your vulnerability management process to assess mean time to patch for critical Cisco advisories on infrastructure management software. Evaluate whether internal REST API endpoints for administrative platforms are adequately segmented from untrusted network zones. Implement network-layer controls to restrict management plane access to authorized management IP ranges only. Review CWE-306 (Missing Authentication for Critical Function) as a recurring control gap in your vendor assessment criteria. Reference: NIST AC-17 (Remote Access), NIST AC-6 (Least Privilege), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), D3-MFA (Multi-factor Authentication), D3-CH (Credential Hardening).

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Using free tooling: (1) deploy a Sigma rule targeting your syslog-forwarded Secure Workload access logs to permanently alert on HTTP 200/201 responses with no Authorization header against the management API paths (Sigma rule: `condition: keywords | contains: '/openapi/' AND response_code: [200, 201] AND NOT keywords | contains: 'Authorization'`); (2) use osquery on the Secure Workload nodes with a scheduled query against `listening_ports` to alert on any new listener added outside the expected port set; (3) document CWE-306 as a mandatory evaluation criterion in your next vendor security assessment questionnaire for all administrative management platforms, particularly those with multi-tenant architecture.

Evidence: For the post-incident lessons-learned record, preserve: (1) the complete timeline of first vulnerability disclosure (Cisco advisory publication date) to patch completion, to calculate actual MTTP (Mean Time to Patch) for this critical infrastructure component; (2) the network segmentation diagram as it existed at the time of disclosure, annotating whether the Secure Workload management plane API was reachable from untrusted network zones — this directly documents the CWE-306 exposure surface for the post-incident report; (3) the final account audit results and policy diff from Step 4 as evidence of confirmed or ruled-out attacker activity during the exposure window.

Detection Guidance

Query Cisco Secure Workload API and application logs for REST API requests that return Site Admin-level responses without an associated authentication token or session identifier in the request headers. Flag any API call to internal management endpoints originating from an IP not in the authorized management CIDR range. Look for cross-tenant resource access patterns where the source tenant does not match the target tenant in the API path or response payload. Correlate against NIST AU-3 content fields: event type, timestamp, source, outcome. If a SIEM is ingesting Secure Workload logs, build a detection rule for: (HTTP 200 OR 201 response) AND (Site Admin API path) AND (no Authorization header OR no session token). Alert on any Site Admin privilege action that has no corresponding authentication event within the same session window. D3-SFA (System File Analysis) and D3-LAM (Local Account Monitoring) apply for post-exploitation indicator hunting. No public IOCs or exploit code have been confirmed at this time; behavioral detection is the primary available method.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1078.004** — Cloud Accounts
- **T1548** — Abuse Elevation Control Mechanism

NIST-800-53R5

- **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-6** — Least Privilege

- **CM-6** — Configuration Settings
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **6.1** — Establish an Access Granting Process
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

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
T1190	Exploit Public-Facing Application	Initial-Access
T1078.004	Cloud Accounts	Defense-Evasion
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation

Sources

Source	URL	Tier
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
	https://cyberpress.org/cisco-secure-workload-flaw/	T3
	https://cybersecuritynews.com/best-data-security-companies/	T3
	https://gbhackers.com/best-cloud-security-solutions/	T3
CVE-2026-20223 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20223	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1

Generated 2026-05-21 06:59 UTC by TJS Security Command Center