INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 06:49 UTC

Cisco Patches Four Critical Vulnerabilities in ISE and Webex (RCE, Path Traversal, Impersonation)

CVE VULNERABILITY | CRITICAL | CVSS 9.9

SCC Item ID	SCC-CVE-2026-0045
Type	CVE Vulnerability
Severity	CRITICAL
CVSS Base Score	9.9
Affected Products	Cisco Identity Services Engine (ISE); Cisco Webex, specific versions not confirmed from available source data
Published	22 hours ago
Discovery Source	Serper

Executive Summary

Cisco disclosed critical vulnerabilities in Identity Services Engine (ISE) and Webex, with the highest scoring CVSS 9.9. ISE flaws allow unauthenticated remote code execution and path traversal; Webex flaws enable user impersonation. Organizations running these products face risk of full system compromise and unauthorized access to network access control infrastructure. Patches are available; apply within 24-48 hours.

Technical Analysis

Cisco ISE and Webex are affected by critical-severity flaws. ISE vulnerabilities map to CWE-94 (code injection enabling RCE) and CWE-22 (path traversal), with a CVSS 9.9 vector allowing unauthenticated or low-privileged remote code execution. Webex flaws introduce user impersonation risk. MITRE ATT&CK techniques T1190 (Exploit Public-Facing Application) and T1059 (Command and Scripting Interpreter) apply. Specific CVE identifiers and affected version ranges are detailed in the Cisco Security Advisory cisco-sa-ise-rce-traversal-8bYndVrZ; consult that advisory directly before applying patches to confirm version compatibility and patch applicability.

Action Checklist

1. Step 1: Containment, Identify all Cisco ISE and Webex deployments in your environment. Restrict network access to ISE administrative interfaces to trusted management networks only. If ISE is

internet-facing, immediately restrict administrative interface access and prioritize patch deployment (target: within 24 hours). Coordinate with business continuity to manage any necessary offline maintenance windows.

2. Step 2: Detection, Review ISE and Webex access logs for anomalous authentication attempts, unexpected file access patterns, or command execution activity. Query SIEM for events matching T1190 (exploitation of public-facing application) and T1059 (script interpreter invocation) on hosts running ISE. Monitor for unexpected API authentication events to admin endpoints, file system modifications to policy directories, and certificate or privilege policy changes without corresponding change tickets. Check Cisco PSIRT for updated IOC patterns as threat intelligence becomes available.

3. Step 3: Eradication, Apply patches published in Cisco Security Advisory cisco-sa-ise-rce-traversal-8bYndVrZ for ISE. Apply corresponding Cisco Webex patches per the relevant Cisco advisory. Confirm affected version ranges in the advisory before applying to avoid compatibility issues. Engage change control and test patches in a staging environment before production deployment.

4. Step 4: Recovery, After patching, validate ISE policy enforcement is functioning correctly. Review ISE session logs for any unauthorized policy changes or certificate additions made prior to patching. Confirm Webex meeting integrity controls are operating as expected. Monitor ISE for post-patch anomalies for at least 72 hours.

5. Step 5: Post-Incident, Assess whether ISE administrative interfaces were unnecessarily exposed to untrusted networks. Review network segmentation controls isolating NAC infrastructure. Evaluate whether privileged access to ISE and Webex admin functions requires additional MFA enforcement. Document gaps and update patch SLA policies for CVSS 9.0+ advisories to prioritize deployment within 24-48 hours.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance immediately if ISE Change Audit logs reveal unauthorized policy modifications, certificate additions, or new admin account creation during the exposure window, as this indicates ISE compromise with potential NAC bypass — an event that may constitute a reportable breach if regulated endpoint data traverses the network access control plane.
Recovery Notes	Post-patch, monitor ISE Live Logs (Operations > RADIUS > Live Logs) continuously for 72 hours for authentication policy violations, unexpected NAC bypass events, or endpoints being granted access under policy rules that should not apply — these patterns indicate either residual attacker persistence or policy tampering that survived patching. Verify all ISE node certificates in the Internal CA store against a known-good inventory, as an attacker exploiting the RCE to plant a rogue trusted certificate could maintain a persistent man-in-the-middle position on 802.1X-authenticated network segments even after patching. For Webex, monitor Admin Audit logs for anomalous meeting join events or admin privilege escalations for at least 7 days post-patch given the impersonation flaw's potential for session token abuse that may outlast the patch window.

Forensic Artifacts	ISE application log /opt/CSCOcpm/logs/ise-psc.log: Contains HTTP request records including URI paths — the path traversal exploitation (T1083) would leave URI-encoded sequences ('../', '%2e%2e', '%252f') in requests to admin endpoints; unauthenticated RCE attempts would appear as POST requests to API or admin endpoints from non-management source IPs receiving 2xx responses. | ISE Change Configuration Audit report (Operations > Reports > Audit > Change Configuration Audit): The highest-value artifact for determining post-exploitation impact — an attacker achieving RCE on ISE would target Authorization Policy rules, Network Device Groups, and Trusted Certificate Store to enable NAC bypass or persistent access; any changes from unknown admin accounts or unexpected IP addresses during the exposure window are critical findings. | ISE filesystem directories /opt/CSCOcpm/webapps/ and /opt/CSCOcpm/portal/: Unauthenticated RCE exploits against Java-based web applications (ISE runs on a Tomcat stack) characteristically result in webshell deployment (.jsp files) in the web application root — enumerate all .jsp and .war files and compare modification timestamps against the last known-good patch date. | Webex Admin Hub Audit Event log (exportable via Webex Admin Hub or REST API GET /v1/adminAudit/events): The impersonation flaw would surface as session events where the authenticated principal identity does not match the user account the session is operating as — look for login events with mismatched 'actorId' and 'targetId' fields, or meeting join events where participant email does not match the registered account's domain. | Network firewall and/or perimeter proxy logs for ISE admin interface ports (443, 8443, 9060): Source IPs, request volumes, and HTTP response codes for traffic to ISE admin ports during the exposure window establish the external attack surface and can confirm whether exploitation was attempted or successful — specifically flag any non-management-network source IPs receiving HTTP 200/201 responses on ERS API port 9060, which is the likely unauthenticated RCE entry point.

Per-Action IR Details

Step 1: Containment — Identify all Cisco ISE and Webex deployments in your environment. Restrict network access to ISE administrative interfaces to trusted management networks only. If ISE is internet-facing, isolate it behind a firewall or take it offline until patched.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run 'nmap -p 443,80,8443,9060 --open -sV' to identify ISE admin portal exposure (default ports 443/8443 for Admin GUI, 9060 for ERS API). Use iptables or Windows Firewall to restrict ISE admin interface access: 'iptables -I INPUT -p tcp --dport 443 -s -j ACCEPT && iptables -I INPUT -p tcp --dport 443 -j DROP'. For ISE nodes, disable ERS and Open API interfaces via ISE Admin GUI under Administration > System > Settings if not actively required.

Evidence: Before restricting access, capture a full netstat snapshot from ISE nodes ('netstat -antp' on Linux-based ISE appliance) to document all active TCP sessions on ports 443, 8443, 9060, and 8905. Export ISE Admin Audit logs from Administration > Logging > Message Catalog filtered to the past 30 days — these record all admin GUI logins, REST API calls, and configuration changes. Capture current ISE node list and their IP assignments from Administration > Deployment before any isolation action to preserve the pre-containment topology baseline.

Step 2: Detection — Review ISE and Webex access logs for anomalous authentication attempts, unexpected file access patterns, or command execution activity. Query SIEM for events matching T1190 (exploitation of public-facing application) and T1059 (script interpreter invocation) on hosts running ISE. Specific IOC patterns are not publicly available at this time; monitor Cisco's advisory for threat intelligence updates.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: For ISE RCE detection without SIEM: SSH to ISE CLI and run 'show logging application ise-psc.log tail 1000' — look for unexpected Java process spawns, shell invocations, or HTTP 200 responses to unusual URI paths (the path traversal component means look for '..', '%2e%2e', or absolute paths in request URIs in /opt/CSCOcpm/logs/ise-psc.log). For Webex impersonation, query Webex Admin Hub audit logs via API: GET https://webexapis.com/v1/adminAudit/events filtering on eventType 'login' with mismatched userAgent strings or logins from unexpected IP ranges. Deploy this Sigma rule concept manually: grep ISE access logs for HTTP requests where the URI contains directory traversal sequences ('grep -E "\.\./|%2e%2e%2f|%252e" /opt/CSCOcpm/logs/access.log').

Evidence: Collect ISE application logs from /opt/CSCOcpm/logs/ise-psc.log and /opt/CSCOcpm/logs/guest-access.log before any log rotation occurs — ISE defaults to 7-day log retention. For the unauthenticated RCE vector, look for HTTP POST/GET requests to ISE admin endpoints (ports 443/8443) originating from IPs not in your management ACL, particularly those receiving HTTP 200/201 responses. For path traversal, extract web server access logs at /opt/CSCOcpm/logs/catalina.out and search for URI-encoded traversal sequences. On Webex, pull Admin Audit Event logs showing session token issuance events where the authenticated identity does not match the initiating user's registered email domain — this is the signature artifact of the impersonation flaw.

Step 3: Eradication — Apply patches published in Cisco Security Advisory cisco-sa-ise-rce-traversal-8bYndVrZ for ISE. Apply corresponding Cisco Webex patches per Cisco's advisory for impersonation flaws. Confirm affected version ranges in the advisory before applying to avoid compatibility issues. Specific patch IDs and version upgrade paths require direct advisory review.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), 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: Before patching ISE, take a VM snapshot or backup via 'backup repository ise-config encryption-key plain ' from ISE CLI to enable rollback. Verify patch integrity by comparing the downloaded ISE patch file SHA-512 hash against the value published in cisco-sa-ise-rce-traversal-8bYndVrZ before installation — do not skip this step given the RCE severity. For Webex (SaaS), confirm your Webex Control Hub admin console reflects the patched version under Settings > Updates; Cisco typically pushes Webex SaaS patches automatically, but tenant admins must verify propagation. Post-patch, run 'show version' from ISE CLI to confirm the patched build string matches the advisory's fixed release.

Evidence: Before applying the ISE patch, image the ISE node filesystem or capture a snapshot of /opt/CSCOcpm/ to preserve any webshell or dropped file artifacts the RCE vulnerability may have been used to plant — specifically check /opt/CSCOcpm/webapps/ and /opt/CSCOcpm/portal/ directories for unexpected .jsp, .war, or .sh files not present in a clean ISE installation manifest. Document the exact ISE version string from 'show version' pre- and post-patch to establish a verified remediation timestamp for audit and potential regulatory reporting purposes.

Step 4: Recovery — After patching, validate ISE policy enforcement is functioning correctly. Review ISE session logs for any unauthorized policy changes or certificate additions made prior to patching. Confirm Webex meeting integrity controls are operating as expected. Monitor ISE for post-patch anomalies for at least 72 hours.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-9 (Protection of Audit Information), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Validate ISE policy enforcement by running a test 802.1X authentication from a known endpoint and confirming the expected Authorization Policy result in ISE Live Logs (Operations > RADIUS > Live Logs) — a mismatch indicates policy tampering. To audit unauthorized certificate additions, navigate to Administration > System > Certificates > Certificate Authority > Internal CA and export the full trusted certificate list, then diff against your last known-good certificate inventory. For Webex recovery validation, create a test meeting as a standard user and confirm you cannot join as or impersonate another registered user — this directly tests the impersonation flaw remediation. Use osquery on the ISE host ('SELECT * FROM file WHERE path LIKE "/opt/CSCOcpm/webapps/%" AND type = "regular"') to enumerate web application files and compare against a clean baseline.

Evidence: Pull ISE Change Audit logs (Operations > Reports > Audit > Change Configuration Audit) for the 30-day window before patch application — filter for changes to Authentication Policies, Authorization Policies, Network Device Groups, and Certificate Stores, which are the high-value targets an attacker achieving RCE on ISE would modify to establish persistence or pivot to NAC bypass. For Webex, export meeting participant history from Admin Hub for meetings held during the exposure window and flag any participant records where the display name or email domain does not match your organization's registered user roster.

Step 5: Post-Incident — Assess whether ISE administrative interfaces were unnecessarily exposed. Review network segmentation controls isolating NAC infrastructure. Evaluate whether privileged access to ISE and Webex admin functions requires additional MFA enforcement. Document gaps and update patch SLA policies for CVSS 9.0+ advisories.

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 AC-2 (Account Management), NIST SC-7 (Boundary Protection), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: To assess ISE exposure, run Shodan queries for 'cisco ise port:443,8443,9060' against your public IP ranges to determine if ISE admin interfaces were indexed — this is free via Shodan's web interface. For MFA enforcement on ISE admin access without enterprise IAM budget, configure ISE's built-in RADIUS-based admin authentication to require a TOTP second factor using an open-source RADIUS server (FreeRADIUS with Google Authenticator PAM module) as the external identity source. To formalize CVSS 9.0+ patch SLA, create a documented policy requiring patch application within 72 hours of advisory publication for Critical-severity Cisco NAC/identity infrastructure, given ISE's role as the network access control plane.

Evidence: For the lessons-learned record, document the full timeline from Cisco advisory publication (cisco-sa-ise-rce-traversal-8bYndVrZ release date) to your patch completion timestamp per ISE node — this delta is your empirical patch latency for Critical advisories and serves as the baseline for SLA policy setting. Preserve the ISE Change Configuration Audit log export from Step 4 as the evidentiary record of pre-patch unauthorized changes, retaining per NIST AU-11 (Audit Record Retention) requirements. Document ISE node network exposure state (internet-facing vs. management-network-only) as of the advisory date to support any future regulatory inquiry regarding exposure window.

Detection Guidance

Until Cisco PSIRT releases specific IOC patterns, detection focus should be behavioral. For ISE: monitor authentication logs for unexpected API calls to administrative endpoints, privilege escalation events, and file system access outside expected policy directories. Monitor for file system modifications to configuration/policy directories, certificate policy changes without corresponding change tickets, and any process execution on ISE appliances outside known maintenance windows. For Webex: review meeting and identity logs for sessions attributed to accounts that did not originate them. In your SIEM, correlate T1190 indicators (unusual inbound connections to ISE admin ports) with T1059 indicators (unexpected process or script execution on ISE hosts).

Set alerts for T1190+T1059 correlation on ISE-related infrastructure. Check Cisco's advisory and Cisco PSIRT for updated threat intelligence as exploitation activity may be reported after initial disclosure.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter

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
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-10** — Information Input Validation
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

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
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
	https://thehackernews.com/2026/04/cisco-patches-four-critical-ident...	T3
Cisco Identity Services Engine Remote Code Execution and Path ...	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
Cisco patches critical bugs in Webex, ISE | news - SC Media	https://www.scworld.com/news/cisco-patches-critical-bugs-in-webex-ise	T3
Cisco Patches Critical Vulnerabilities in Webex, ISE - SecurityWeek	https://www.securityweek.com/cisco-patches-critical-vulnerabilities...	T3
Cisco Patches Four Critical Identity Services, Webex Flaws Enabling ...	https://x.com/TheCyberSecHub/status/2044747533583589641	T3

Generated 2026-04-17 06:49 UTC by TJS Security Command Center