INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 18:53 UTC

# Cisco ISE Carries a Two-Vector Risk: Unauthenticated Credential Exposure Feeds Authenticated RCE, No Full Patch Until August

**CVE VULNERABILITY** | **CRITICAL** | CVSS 9.5

| | |
|---|---|
| **SCC Item ID** | SCC-CVE-2026-0322 |
| **Type** | CVE Vulnerability |
| **CVE ID** | CVE-2026-20181, CVE-2026-20190 |
| **Severity** | CRITICAL |
| **CVSS Base Score** | 9.5 |
| **Affected Products** | Cisco Identity Services Engine (ISE) and ISE Passive Identity Connector (ISE-PIC), all releases prior to 3.3 Patch 11, 3.4 Patch 6, 3.5 Patch 3/4 |
| **Published** | 2026-06-17T16:00:00+00:00 |
| **Discovery Source** | Rss:T1 Psirt |

## Executive Summary

Cisco disclosed two vulnerabilities in Identity Services Engine (ISE) on June 17, 2026, that chain together into a critical attack path: an unauthenticated attacker can harvest hashed administrative credentials and then execute arbitrary code on the ISE appliance. ISE is a network access control platform; compromise gives an attacker the ability to manipulate network policy, revoke or forge access decisions, and move laterally across the enterprise. Full patches are not available for ISE 3.5 until August 2026, leaving organizations on that release in an extended exposure window with no workaround.

## Technical Analysis

Cisco Security Advisory cisco-sa-ise-multi-G5WP8vv covers two vulnerabilities disclosed June 17, 2026. CVE-2026-20181 (CVSS 9.1, critical) is an authenticated RCE flaw rooted in path traversal (CWE-22) and improper authorization (CWE-285); an attacker with administrative credentials can traverse restricted paths to execute arbitrary commands on the underlying OS. CVE-2026-20190 (CVSS 7.5, high) is an unauthenticated information disclosure flaw rooted in improper input validation (CWE-20) and insufficiently protected credentials (CWE-522); it exposes hashed credentials to an unauthenticated remote attacker. The chained attack path is the primary risk: exploit CVE-2026-20190 to retrieve hashed credentials, crack or relay them, then exploit CVE-2026-20181 for RCE. Both ISE and ISE Passive Identity Connector (ISE-PIC) are affected across all releases prior to: 3.3 Patch 11, 3.4 Patch 6, 3.5 Patch 3 (RCE partial), 3.5 Patch 4 (full RCE fix, August 2026).

No workarounds exist for either CVE. MITRE techniques relevant to this chain include T1190 (Exploit Public-Facing Application), T1552 (Unsecured Credentials), T1110.002 (Password Cracking), T1078.002 (Valid Domain Accounts), T1505.003 (Web Shell), and T1059 (Command and Scripting Interpreter). Telemetry from threat research indicates active adversarial interest in this attack surface predating public disclosure.

## Action Checklist

1. Step 1: Containment, Immediately identify all ISE and ISE-PIC nodes running releases prior to 3.3 Patch 11, 3.4 Patch 6, or 3.5 Patch 3/4. Restrict administrative interface access (ERS API, Admin GUI) to trusted management network segments via ACL or firewall rule. Remove any ISE admin interface exposure to the internet or untrusted VLANs. If ISE 3.5 is in use, treat the appliance as operating under extended exposure until August 2026 patch availability, apply compensating network controls immediately. Reference: Cisco advisory cisco-sa-ise-multi-G5WP8vv.
2. Step 2: Detection, Query ISE runtime logs and syslog output for anomalous unauthenticated requests to credential-related API endpoints (indicators of CVE-2026-20190 exploitation). Review administrative session logs for unexpected logins or sessions originating from unusual source IPs or at unusual hours (T1078.002). Check for unexpected file creation or process execution events on ISE nodes (T1505.003, T1059). Correlate with network flow data for outbound connections from ISE appliances to external IPs. Cross-reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) logging practices to confirm log completeness. Safeguard CIS 8.2 (Collect Audit Logs) should be validated, confirm ISE audit logging is enabled and forwarding to your SIEM.
3. Step 3: Eradication, Apply available patches per release track: ISE 3.3 → Patch 11; ISE 3.4 → Patch 6; ISE 3.5 → Patch 3 immediately (partial RCE coverage), then Patch 4 upon August 2026 availability (full RCE fix). Obtain patches from Cisco Software Download via your Cisco service contract; if you do not have an active contract, contact Cisco to obtain patches or explore emergency support options. After patching, rotate all ISE administrative account credentials and any credentials potentially exposed through CVE-2026-20190 exploitation (D3-CRO: Credential Rotation). Audit ISE admin accounts for unauthorized additions per NIST AC-2 (Account Management) and CIS 5.1 (Establish and Maintain an Inventory of Accounts).
4. Step 4: Recovery, After patching, verify ISE administrative interface returns expected behavior and no unauthorized accounts or configurations persist. Re-enable any access policies tightened during containment only after patch verification. Monitor ISE logs for 30 days post-patch for residual indicators of compromise: unexpected admin sessions, anomalous policy changes, or outbound connection attempts from ISE nodes. Validate that audit logging is intact per NIST AU-9 (Protection of Audit Information), confirm logs were not tampered during any exploitation window.
5. Step 5: Post-Incident, This vulnerability chain exposes a control gap in administrative credential protection for network access control infrastructure. Conduct a review of ISE admin account privilege levels against NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Verify MFA is enforced on all ISE administrative access per CIS 6.5 (Require MFA for Administrative Access) and D3-MFA. Review your patch SLA for critical network infrastructure, ISE nodes should be on a tracked patch cycle per CIS 7.1 (Establish and Maintain a Vulnerability Management Process). Document the August 2026 ISE 3.5 full-patch deadline as a tracked risk item with compensating controls formally recorded.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to CISO and legal/compliance immediately if ISE audit logs or network flows show evidence that CVE-2026-20190 credential harvest attempts were successful (i.e., harvested hashes subsequently used for authenticated sessions) or that CVE-2026-20181 RCE occurred on an ISE node, as this constitutes compromise of the network access control plane with potential lateral movement scope across the entire enterprise, and may trigger breach notification obligations if ISE-managed network segments process PII, PHI, or PCI-scoped data. |
| **Recovery Notes** | After patching and credential rotation are confirmed, restore ISE to full policy enforcement only after a side-by-side diff of current Policy Sets against the last known-good configuration backup confirms no unauthorized authorization rules were inserted during the exploitation window — pay particular attention to any rules that bypass posture assessment or grant elevated SGT (Security Group Tag) assignments. Monitor ISE Admin Audit logs and ERS API access logs daily for the first 30 days post-patch, specifically for admin sessions from non-management-VLAN source IPs or API calls using credentials that were in scope for CVE-2026-20190 exposure, as adversaries may have exfiltrated hashes for offline cracking and could return with cracked credentials after patch deployment. For ISE 3.5 environments, maintain the management-VLAN ACL containment control and formally document it as a compensating control in the risk register until the full RCE fix in Patch 4 is available and applied in August 2026. |
| **Forensic Artifacts** | ISE ERS API access log entries (syslog facility, default forwarded from ISE to syslog server) showing unauthenticated HTTP requests to credential-related REST endpoints — specifically 400/401/200-series responses to ERS API paths under /ers/config/ from source IPs outside the management VLAN, which are the direct fingerprint of CVE-2026-20190 exploitation attempts \| ISE Admin Audit log (Operations > Reports > Audit > Change Configuration Audit, exportable as CSV) showing any administrative logins or configuration changes — particularly new admin account creations, policy rule insertions, or RADIUS/TACACS configuration changes — occurring in the timeframe between the earliest detected ERS anomaly and containment, which would indicate successful credential use post-harvest \| OS-level process execution records from the ISE appliance underlying Linux OS — specifically entries in `/var/log/messages` or `/var/log/audit/audit.log` (if auditd is running) showing processes spawned outside normal ISE service process tree (e.g., unexpected bash, python, or curl invocations), which are artifacts of CVE-2026-20181 authenticated RCE exploitation \| Network flow data (NetFlow/IPFIX/sFlow) for outbound TCP connections originating from ISE node management IPs to external or non-datacenter destinations on non-standard ports, which would indicate a reverse shell or C2 beacon established via RCE payload execution following the credential-harvest-to-RCE attack chain \| ISE configuration backup diff (compare pre-incident backup against post-incident export using `diff` on extracted XML) specifically examining the Authorization Policy and Network Device Group sections for unauthorized rules that could persist as a backdoor access path even after credentials are rotated and patches are applied |

### Per-Action IR Details

**Step 1: Containment — Immediately identify all ISE and ISE-PIC nodes running releases prior to 3.3 Patch 11, 3.4 Patch 6, or 3.5 Patch 3/4. Restrict administrative interface access (ERS API, Admin GUI) to trusted management network segments via ACL or firewall rule. Remove any ISE admin interface exposure to the**

**internet or untrusted VLANs. If ISE 3.5 is in use, treat the appliance as operating under extended exposure until August 2026 patch availability — apply compensating network controls immediately. Reference: Cisco advisory cisco-sa-ise-multi-G5WP8vv.**

**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:** On the upstream perimeter firewall or switch ACL, immediately apply an explicit deny for all source IPs outside the designated management VLAN to TCP ports 443 (Admin GUI) and 9060/9061 (ERS API) on each ISE node IP. Verify the block using: `curl -k --max-time 5 https:///ers/config/` from an untrusted host — a timeout or connection refused confirms the ACL is effective. For ISE-PIC, also block port 8443 if the Passive ID web interface is exposed. Document blocked IPs and timestamps for chain-of-custody.

**Evidence:** Before implementing any ACL or firewall rule changes that drop live traffic to ISE, capture: (1) full `netstat -an` / `ss -tnp` output from the ISE CLI (`show socket` or SSH to the underlying OS if accessible) to record all active TCP connections to the Admin GUI and ERS API ports at time of containment; (2) ISE runtime logs from `/var/log/messages` and the Cisco ISE Admin audit log (`Operations > Reports > Audit > Change Configuration Audit`) to preserve any pre-containment unauthenticated requests to ERS credential endpoints that constitute CVE-2026-20190 exploitation evidence; (3) a network flow snapshot (NetFlow/IPFIX or a brief tcpdump on the ISE management interface) capturing source IPs communicating with ports 443, 9060, and 9061 in the 24–72 hours prior to isolation.

**Step 2: Detection — Query ISE runtime logs and syslog output for anomalous unauthenticated requests to credential-related API endpoints (indicators of CVE-2026-20190 exploitation). Review administrative session logs for unexpected logins or sessions originating from unusual source IPs or at unusual hours (T1078.002). Check for unexpected file creation or process execution events on ISE nodes (T1505.003, T1059). Correlate with network flow data for outbound connections from ISE appliances to external IPs. Cross-reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) logging practices to confirm log completeness. Safeguard CIS 8.2 (Collect Audit Logs) should be validated — confirm ISE audit logging is enabled and forwarding to your SIEM.**

**NIST Phase:** Detection Analysis

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

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

**Compensating:** Without a SIEM, parse ISE syslog directly: `grep -E '(ERS|api|credential|unauthenticated|401|403)' /var/log/cisco/ise/ise-psc.log | awk '{print $1,$2,$3,$NF}' | sort | uniq -c | sort -rn` to surface anomalous ERS API hits. For admin session anomalies, export the ISE Admin Audit report (Operations > Reports > Audit > Admin Users) as CSV and filter in Excel or `awk` for sessions outside business hours or from non-management-VLAN source IPs. Use Wireshark with display filter `tcp.port == 9060 || tcp.port == 9061` on a span/mirror port to capture live ERS API traffic and identify unauthenticated credential harvest attempts in real time.

**Evidence:** This is a read-and-analyze step that does not alter live state, so no volatile capture is required before beginning analysis. However, evidence to collect and preserve during this step includes: (1) ISE syslog entries (default path `/var/log/cisco/ise/ise-psc.log` and `ise-system.log`) covering the full exposure window back to the last known-clean state; (2) ISE Admin Audit log exports showing all administrative logins, configuration changes, and API calls — specifically any ERS API calls authenticated with credentials that should not have been in use; (3) ISE Guest and Sponsor portal access logs if the credential exposure via CVE-2026-20190 affected service accounts used for portal auth; (4) network flow records (NetFlow/sFlow) for outbound connections from ISE node IPs to external destinations, which would indicate a successful RCE payload establishing C2 via CVE-2026-20181 post-credential-harvest.

**Step 3: Eradication — Apply available patches per release track: ISE 3.3 → Patch 11; ISE 3.4 → Patch 6; ISE 3.5 → Patch 3 immediately (partial RCE coverage), then Patch 4 upon August 2026 availability (full RCE fix). Obtain patches from Cisco Software Download via your Cisco service contract. After patching, rotate all ISE administrative account credentials and any credentials potentially exposed through CVE-2026-20190 exploitation (D3-CRO: Credential Rotation). Audit ISE admin accounts for unauthorized additions per NIST AC-2 (Account Management) and CIS 5.1 (Establish and Maintain an Inventory of Accounts).**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

**Compensating:** Before patching, take a configuration backup via ISE CLI: `backup ise-config location ftp://... encryption-key plain ` to preserve pre-patch state for forensic comparison. For credential rotation without an enterprise PAM tool, generate new passwords using `openssl rand -base64 24` for each ISE admin account, update directly in ISE Administration > Identity Management > Identities, and record the rotation event with timestamp in your incident log. To audit for unauthorized admin accounts added via CVE-2026-20190 exploitation, export the full admin user list from ISE GUI (Administration > Identity Management > Identities > Users, filter by User Groups = 'Super Admin' and 'Admin') and diff against your last known-good account inventory.

**Evidence:** Before applying any patch or rotating credentials — both of which alter live system state and will overwrite volatile artifacts — capture: (1) a full memory image of the ISE appliance OS if the platform supports it (ISE runs on a hardened Linux base; use `dd` or `LiME` kernel module if accessible via support tunnel to preserve any in-memory indicators of CVE-2026-20181 RCE payload execution); (2) the current running process list (`ps auxf` via ISE CLI `show process`) and open file handles (`lsof -p `) to document any anomalous processes spawned via RCE before the patch closes the vector; (3) the `/etc/passwd`, `/etc/shadow` (hashed), and `/home` directory listing on the ISE OS to detect OS-level backdoor accounts created via RCE; (4) the ISE internal SQLite or Oracle DB admin account table snapshot (exportable via ISE backup) before credential rotation overwrites the current state.

**Step 4: Recovery — After patching, verify ISE administrative interface returns expected behavior and no unauthorized accounts or configurations persist. Re-enable any access policies tightened during containment only after patch verification. Monitor ISE logs for 30 days post-patch for residual indicators of compromise: unexpected admin sessions, anomalous policy changes, or outbound connection attempts from ISE nodes. Validate that audit logging is intact per NIST AU-9 (Protection of Audit Information) — confirm logs were not tampered during any exploitation window.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), NIST AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts)

**Compensating:** To verify ISE integrity post-patch without enterprise tooling: (1) run `show version` and `show patch` via ISE CLI to confirm patch level matches expected 3.3P11 / 3.4P6 / 3.5P3; (2) re-export the admin account list and diff against the pre-patch snapshot captured during eradication to confirm no accounts were re-added; (3) set up a daily cron job on your syslog server to alert on any ISE syslog entries containing 'CONFIG_CHANGE', 'ADMIN_LOGIN', or 'ERS_REQUEST' from source IPs outside the management VLAN: `grep -E '(CONFIG_CHANGE|ADMIN_LOGIN|ERS_REQUEST)' /var/log/ise-syslog.log | grep -v ` — pipe output to email for 30-day monitoring period.

**Evidence:** Recovery actions (re-enabling access policies, restoring normal ISE operation) do not typically destroy volatile evidence if eradication was completed correctly. However, before re-enabling any ISE policy enforcement that was suspended during containment, confirm: (1) the ISE audit log continuity — verify log timestamps are contiguous with no gaps during the exploitation window, which would indicate log tampering via RCE (CVE-2026-20181 execution could have been used to clear or truncate `/var/log/cisco/ise/ise-psc.log`); (2) a comparison of ISE network access policy rules (Policy > Policy Sets export) against your last known-good configuration backup to detect any unauthorized

policy modifications made via the compromised admin interface — specifically, look for new authorization rules granting elevated network access or bypassing posture assessment.

**Step 5: Post-Incident — This vulnerability chain exposes a control gap in administrative credential protection for network access control infrastructure. Conduct a review of ISE admin account privilege levels against NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Verify MFA is enforced on all ISE administrative access per CIS 6.5 (Require MFA for Administrative Access) and D3-MFA. Review your patch SLA for critical network infrastructure — ISE nodes should be on a tracked patch cycle per CIS 7.1 (Establish and Maintain a Vulnerability Management Process). Document the August 2026 ISE 3.5 full-patch deadline as a tracked risk item with compensating controls formally recorded.**

**NIST Phase:** Post Incident

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

**Controls:** NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), 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:** For MFA enforcement on ISE admin access without a commercial MFA solution: configure ISE to authenticate admin logins against an external RADIUS server (ISE supports this natively under Administration > Admin Access > Authentication) and front that RADIUS server with a free TOTP solution such as FreeRADIUS + Google Authenticator PAM module, which is achievable by a 2-person team in under a day. For patch SLA tracking without a vulnerability management platform, maintain a simple tracked spreadsheet with columns: CVE ID, affected ISE version, patch available date, patch applied date, compensating control in place, and risk acceptance owner — flag the August 2026 ISE 3.5 Patch 4 deadline as a calendar-triggered review item with the CISO or system owner as accountable party.

**Evidence:** No volatile evidence capture is required for post-incident activities, as this phase occurs after the environment is restored. The key artifact to produce and retain from this phase is a formal lessons-learned document that includes: (1) a timeline reconstructed from ISE audit logs, syslog, and network flows showing the earliest detectable indicator of CVE-2026-20190 unauthenticated credential harvest attempts (first ERS API anomaly timestamp); (2) a record of whether any harvested credentials were successfully used for authenticated RCE via CVE-2026-20181 (correlated from admin session logs and process execution artifacts captured during eradication); (3) the delta between the Cisco advisory publication date (June 17, 2026) and the organization's containment action date, to quantify exposure window for the risk register and any regulatory reporting obligations.

## Detection Guidance

Focus detection on two distinct phases of the chained attack. Phase 1 (credential harvesting via CVE-2026-20190): look for unauthenticated or pre-authentication HTTP requests to ISE API endpoints that return credential material or generate unusual 200-series responses without a valid session token. Specifically, monitor ISE application logs (/opt/CSCOcpm/logs/) for unexpected API calls from external or non-management IPs. Anomalous volume of requests to credential-related endpoints from a single source IP is a behavioral indicator. Phase 2 (RCE via CVE-2026-20181): look for path traversal sequences (e.g., '../', '%2e%2e%2f', URL-encoded variants) in ISE web server access logs. Monitor for unexpected process spawning or file writes on ISE appliances, this is not standard ISE behavior and warrants immediate investigation. In your SIEM, create correlation rules mapping MITRE T1190 (external exploit attempt against ISE admin interface) chained with T1078.002 (successful admin logon from unusual IP or time) followed by T1059 (command execution). D3-SFA (System File Analysis) should be applied: monitor ISE system files and configuration directories for unauthorized modification. D3-LAM (Local Account Monitoring) should flag any new local admin account creation post-exploit. If network flow telemetry is available, flag outbound connections from ISE node IPs to non-Cisco,

non-management destinations, ISE appliances have a narrow legitimate outbound communication profile.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| URL | `Path traversal patterns in ISE web logs: sequences containing '../', '%2e%2e%2f', or URL-encoded equivalents in requests to ISE admin endpoints` | Behavioral IOC for CVE-2026-20181 exploitation attempt via path traversal (CWE-22) against ISE administrative interface | MEDIUM |
| URL | `Unauthenticated requests returning HTTP 200 to ISE credential-related API endpoints from non-management source IPs` | Behavioral IOC for CVE-2026-20190 credential harvesting phase; pre-authentication access to endpoints that should require a valid session | MEDIUM |

## Framework Mappings

### MITRE-ATTACK

- **T1505.003** — Web Shell
- **T1078.002** — Domain Accounts
- **T1068** — Exploitation for Privilege Escalation
- **T1110.002** — Password Cracking
- **T1083** — File and Directory Discovery
- **T1552** — Unsecured Credentials
- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter
- **T1078** — Valid Accounts

### NIST-800-53R5

- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning

- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation

### OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection

### CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

### HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

### ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

### SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1505.003 | Web Shell | Persistence |
| T1078.002 | Domain Accounts | Defense-Evasion |
| T1068 | Exploitation for Privilege Escalation | Privilege-Escalation |
| T1110.002 | Password Cracking | Credential-Access |

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1083 | File and Directory Discovery | Discovery |
| T1552 | Unsecured Credentials | Credential-Access |
| T1190 | Exploit Public-Facing Application | Initial-Access |
| T1059 | Command and Scripting Interpreter | Execution |
| T1078 | Valid Accounts | Defense-Evasion |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Cisco Security Advisory** | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri... | T3 |
| | https://www.linkedin.com/pulse/cisco-patches-critical-webex-identit... | T3 |
| | https://www.cybersecuritydive.com/news/threat-actor-zero-day-flaws-... | T3 |
| | https://www.crowe.com/ae/news/critical-vulnerabilities | T3 |
| **Cisco Identity Services Engine Remote Code Execution and ...** | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri... | T3 |
| **NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-20181, CVE-2026-20190 | T1 |
| **Cisco Security Advisory** | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri... | T1 |



Generated 2026-06-17 18:53 UTC by TJS Security Command Center