INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-01 14:59 UTC

Cisco Catalyst Center Arbitrary File Read Joins Broader Wave of Unauthenticated Cisco Exploits

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0378
Type	CVE Vulnerability
CVE ID	CVE-2026-20191
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Cisco Catalyst Center, hardware appliances, virtual appliances on AWS, Azure, and VMware ESXi, releases 3.1 and 2.3.7
Published	2026-07-01T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Cisco disclosed a path traversal vulnerability (CVE-2026-20191) in Catalyst Center, its centralized network management and automation platform, affecting hardware and virtual appliances on AWS, Azure, and VMware ESXi running releases 3.1 and 2.3.7. An unauthenticated remote attacker can read arbitrary files from affected systems without credentials. Cisco PSIRT confirmed no active exploitation as of July 1, 2026; however, Catalyst Center's role as a high-privilege network management plane makes it a high-value target, and a documented pattern of Cisco management-plane vulnerabilities being actively weaponized in 2026 (CVE-2026-20128, CVE-2026-20122) elevates the urgency to patch.

Technical Analysis

CVE-2026-20191 is a path traversal vulnerability (CWE-22) in Cisco Catalyst Center affecting all hardware appliances and virtual appliances (AWS, Azure, VMware ESXi) running release 3.1 or 2.3.7. The flaw allows an unauthenticated remote attacker to traverse directory boundaries and read arbitrary files from the underlying system via crafted HTTP requests, without requiring authentication. CVSS base score is 7.5 (High) per the Cisco Security Advisory; the full CVSS vector string was not available in the source data. MITRE ATT&CK techniques mapped: T1190 (Exploit Public-Facing Application), T1083 (File and Directory Discovery), T1552 (Unsecured Credentials). No workaround exists. Remediation requires upgrade to version 3.1.6 GSMU200 (hardware/cloud appliances) or 2.3.7.11-VA GSMU100 (VMware ESXi). The vulnerability is not listed in the CISA Known Exploited Vulnerabilities catalog as of the item date. EPSS score was not available in the source

data. This CVE is contextually linked to a broader 2026 pattern of Cisco management-plane exploitation: CVE-2026-20128 and CVE-2026-20122 were reported as actively exploited (per Helpnetsecurity), and Cisco Unified CM flaws were reported as exploited in the wild (per The Hacker News and Computing). Source: Cisco Security Advisory cisco-sa-catc-file-read-wLH2vf8X (T1); NVD CVE-2026-20191 (T1).

Action Checklist

1. Step 1: Containment, Immediately identify all Cisco Catalyst Center deployments (hardware appliances, AWS, Azure, VMware ESXi) running release 3.1 or 2.3.7. Restrict network access to the Catalyst Center management interface to trusted administrative source IPs only, using perimeter firewall or security group rules, until patching is complete. Reference: Cisco Security Advisory cisco-sa-catc-file-read-wLH2vf8X.
2. Step 2: Detection, Review web server and application access logs on Catalyst Center for HTTP requests containing path traversal sequences (e.g., '../', '%2e%2e%2f', '%252e%252e') targeting file system paths, particularly from unauthenticated source IPs. Audit AU-6 (Audit Record Review, Analysis, and Reporting) log sources for anomalous file access patterns. Cross-reference source IPs against known-bad threat intelligence feeds. No public IOCs were identified in the source material.
3. Step 3: Eradication, Apply the vendor-specified patches: upgrade to Cisco Catalyst Center version 3.1.6 GSMU200 (hardware and cloud appliances on AWS/Azure) or version 2.3.7.11-VA GSMU100 (VMware ESXi virtual appliances). No workaround exists per the Cisco advisory; patching is the only remediation. Follow CIS 7.4 (Perform Automated Application Patch Management) and NIST SI-class patching processes.
4. Step 4: Recovery, After patching, verify the installed version matches the target release. Re-enable full management-plane access and confirm Catalyst Center operational health. Review post-patch access logs for continued anomalous requests indicating active exploitation attempts. Validate that access controls restricting management-plane exposure remain in place per AC-17 (Remote Access) and AC-3 (Access Enforcement).
5. Step 5: Post-Incident, Assess whether Catalyst Center's management interface was unnecessarily internet-exposed; implement network segmentation to isolate management-plane systems per AC-4 (Information Flow Enforcement) and CIS 4.4 (Implement and Manage a Firewall on Servers). Conduct a broader review of Cisco management-plane assets in your environment given the documented 2026 exploitation pattern affecting CVE-2026-20128, CVE-2026-20122, and Cisco Unified CM. Review CIS 7.1 (Establish and Maintain a Vulnerability Management Process) to ensure Cisco advisory feeds are included in your vulnerability intake pipeline.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal/compliance if web server access logs show any HTTP 200 responses to path-traversal requests from non-administrative source IPs against the Catalyst Center management interface, as successful unauthenticated file reads from a network management platform may expose network credentials, API keys, or configuration data constituting a reportable data exposure under applicable regulatory frameworks (e.g., PCI DSS Requirement 12.10, HIPAA Breach Notification Rule, or SEC incident disclosure requirements).

Recovery Notes	After applying Cisco patches (3.1.6 GSMU200 or 2.3.7.11-VA GSMU100), monitor Catalyst Center nginx access logs for a minimum of 72 hours for continued path-traversal HTTP requests, which would indicate either patch failure or a threat actor who had established persistence prior to containment. Verify that all managed network devices remain in their expected configuration state within Catalyst Center — an attacker who successfully read sensitive files (e.g., Catalyst Center database credentials, API tokens, or managed-device credentials stored in the platform) may have used those to pivot to downstream network infrastructure, requiring a separate credential rotation exercise for all devices managed by the affected Catalyst Center instance. Retain pre-patch log archives for a minimum of 90 days to support any subsequent forensic investigation or regulatory inquiry.
Forensic Artifacts	Catalyst Center nginx web service access logs at `/var/log/maglev/nginx/access.log` — primary evidence source for CVE-2026-20191 exploitation attempts; filter for HTTP requests containing `../`, `%2e%2e%2f`, `%252e%252e`, or absolute path references (`/etc/`, `/var/`, `/opt/`) with HTTP 200 response codes from unauthenticated (no session cookie or Authorization header) source IPs. | Catalyst Center application-layer logs at `/var/log/maglev/` — secondary evidence capturing internal file-open and file-read operations by the web service process, which would reflect the actual files retrieved if the path traversal succeeded, including potentially sensitive files such as database configuration, API keys, or managed-device credential stores. | OS-level Linux auditd records (`/var/log/audit/audit.log`) on the Catalyst Center appliance — if auditd is enabled with `-a always,exit -F arch=b64 -S open,openat -F success=1` rules, these will log kernel-level file-open syscalls with the calling process UID and the exact file path read, providing ground-truth confirmation of which files an attacker accessed. | Cloud provider access logs (AWS CloudTrail, Azure Monitor/NSG flow logs) for virtual deployments — capture the source IP, timestamp, and API call pattern for any unauthorized access to the Catalyst Center EC2 instance or Azure VM management interface, and identify whether the attacker's source IP made any subsequent API calls to cloud resources using credentials that may have been read from the appliance filesystem. | Catalyst Center managed-device configuration snapshots and credential vault exports — if the path traversal allowed reading of Catalyst Center's internal credential store or device configuration database (SQLite or PostgreSQL files at paths accessible to the web service process), these artifacts establish the blast radius of the compromise and which downstream network devices require credential rotation.

Per-Action IR Details

Step 1: Containment — Immediately identify all Cisco Catalyst Center deployments (hardware appliances, AWS, Azure, VMware ESXi) running release 3.1 or 2.3.7. Restrict network access to the Catalyst Center management interface to trusted administrative source IPs only, using perimeter firewall or security group rules, until patching is complete. Reference: Cisco Security Advisory cisco-sa-catc-file-read-wLH2vf8X.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Isolate affected Catalyst Center management interfaces to prevent unauthenticated arbitrary file read exploitation of CVE-2026-20191 while preserving live state for forensic collection.

Controls: NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: On AWS, update the Catalyst Center EC2 security group inbound rules via AWS CLI: `aws ec2 revoke-security-group-ingress --group-id --protocol tcp --port 443 --cidr 0.0.0.0/0` then re-add only trusted CIDR ranges. On Azure, use `az network nsg rule update` to restrict the NSG associated with the Catalyst Center NIC. On VMware ESXi, apply a host-based firewall rule or vSphere Distributed Switch port-group ACL to permit only admin management VLANs. For hardware appliances, push an ACL to the upstream perimeter switch/firewall restricting

TCP/443 and TCP/80 to a named admin-IP object-group.

Evidence: Before applying firewall or security-group rules that will cut off attacker access, capture: (1) full `netstat -ano` or `ss -tnp` output from the Catalyst Center appliance to document any active TCP sessions on port 443/80 from non-administrative IPs; (2) running process list (`ps auxf` on the appliance OS) to detect any child processes spawned by the web service that could indicate in-progress exploitation; (3) current Catalyst Center application log snapshot from `/var/log/maglev/` and the nginx/apache access logs before session teardown, as live connection state will be lost once ACLs are applied.

Step 2: Detection — Review web server and application access logs on Catalyst Center for HTTP requests containing path traversal sequences (e.g., '../', '%2e%2e%2f', '%252e%252e') targeting file system paths, particularly from unauthenticated source IPs. Audit AU-6 (Audit Record Review, Analysis, and Reporting) log sources for anomalous file access patterns. Cross-reference source IPs against known-bad threat intelligence feeds. No public IOCs were identified in the source material.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Analyze Catalyst Center web service logs for path traversal patterns characteristic of CVE-2026-20191 exploitation, correlating unauthenticated HTTP requests with file-system read artifacts to determine exploitation scope.

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: SSH to the Catalyst Center appliance (or pull logs via SCP) and run: `grep -E '(\.\./|%2e%2e%2f|%252e%252e|%2e%2e/)' /var/log/maglev/nginx/access.log | grep -v ' 401 ' | awk '{print $1, $7, $9}'` to surface unauthenticated traversal attempts with HTTP response codes. Use `awk '$9 == 200' access.log | grep -E '%2e%2e|\.\./'` to isolate successful reads. Write a Sigma rule targeting these URL patterns against the Catalyst Center nginx log source for teams forwarding logs to any SIEM-lite (Graylog, Wazuh). Cross-reference extracted source IPs against free threat intel via `curl https://otx.alienvault.com/api/v1/indicators/IPv4//reputation` using the OTX free API.

Evidence: Volatile evidence to capture before any remediation action: (1) Catalyst Center nginx/web-tier access logs at `/var/log/maglev/nginx/access.log` — these rotate and may be overwritten; archive immediately. (2) Catalyst Center application-layer logs at `/var/log/maglev/` capturing internal file-open operations that would reflect which files were actually read via the traversal. (3) OS-level file access audit records — if Linux auditd is enabled on the appliance, export `ausearch -sc open -ts today` output to capture kernel-level file read events tied to the web service process UID. (4) Active TCP connection table (`ss -tnp state established`) to identify any persistent attacker sessions before containment ACLs drop them.

Step 3: Eradication — Apply the vendor-specified patches: upgrade to Cisco Catalyst Center version 3.1.6 GSMU200 (hardware and cloud appliances on AWS/Azure) or version 2.3.7.11-VA GSMU100 (VMware ESXi virtual appliances). No workaround exists per the Cisco advisory; patching is the only remediation. Follow CIS 7.4 (Perform Automated Application Patch Management) and NIST SI-class patching processes.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Remove CVE-2026-20191 from the environment by applying Cisco-issued patches (3.1.6 GSMU200 for hardware/AWS/Azure; 2.3.7.11-VA GSMU100 for ESXi), the sole remediation per the Cisco advisory cisco-sa-catc-file-read-wLH2vf8X.

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

Compensating: For teams that cannot immediately apply the Cisco GSMU patch through the standard Catalyst Center Software Update workflow, pre-download the GSMU package from Cisco Software Download to a local staging server and verify the SHA-512 checksum published in the advisory before transfer to the appliance. On VMware ESXi, snapshot the Catalyst Center VM (`vim-cmd vmsvc/snapshot.create pre-patch snapshot`) immediately before applying 2.3.7.11-VA GSMU100 to enable rapid rollback without full reimage. Maintain management-interface ACL restrictions from Step 1 throughout the patch window.

Evidence: Before initiating the upgrade (which modifies appliance filesystem and application state, destroying pre-patch file-system evidence): (1) Acquire a full memory dump of the Catalyst Center appliance process space if

forensic investigation of potential prior exploitation is required — use the appliance OS `gcore ` against the web service process or a hypervisor-level memory snapshot for virtual deployments. (2) Archive complete web service logs from `/var/log/maglev/` to an external, write-protected evidence store — the upgrade process may rotate or purge these. (3) For ESXi deployments, export a VM snapshot or OVF export of the pre-patch state before applying 2.3.7.11-VA GSMU100, preserving a forensically consistent image for later analysis. (4) Document the pre-patch version string from the Catalyst Center UI (System > About) or CLI for chain-of-custody records.

Step 4: Recovery — After patching, verify the installed version matches the target release. Re-enable full management-plane access and confirm Catalyst Center operational health. Review post-patch access logs for continued anomalous requests indicating active exploitation attempts. Validate that access controls restricting management-plane exposure remain in place per AC-17 (Remote Access) and AC-3 (Access Enforcement).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Verify Catalyst Center is running 3.1.6 GSMU200 or 2.3.7.11-VA GSMU100, confirm management-plane health, and validate that containment ACLs established in Step 1 remain enforced before restoring full operational access.

Controls: NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Verify patched version via Catalyst Center CLI: `maglev package list | grep catalyst-center` and confirm output matches 3.1.6 GSMU200 or 2.3.7.11-VA GSMU100. Run a targeted path-traversal probe from a controlled admin host using `curl -sk 'https:///api/v1/../../../../etc/passwd' -o /tmp/probe.txt && cat /tmp/probe.txt` — a patched system should return a 400 or 404, not file contents. Continue grep-based log monitoring from Step 2 for 72 hours post-patch to detect any exploitation attempts that pre-dated ACL enforcement. Re-validate firewall/security-group rules using AWS `aws ec2 describe-security-groups` or Azure `az network nsg rule list` to confirm trusted-IP restrictions are still in effect.

Evidence: Post-patch monitoring artifacts to retain as recovery verification evidence: (1) Post-patch nginx access log snapshot from `/var/log/maglev/nginx/access.log` for 72 hours, specifically filtered for any continued path-traversal sequences from external IPs — presence after patching indicates either patch failure or a parallel attacker who had already established a foothold. (2) Catalyst Center system health API response (`GET /api/v1/diagnostics/system/health`) showing all services in healthy state post-upgrade. (3) Screenshot or exported output of the version confirmation from System > About in the Catalyst Center UI, timestamped, for change management records. (4) Firewall/security-group rule export post-recovery to document the final access-control posture.

Step 5: Post-Incident — Assess whether Catalyst Center's management interface was unnecessarily internet-exposed; implement network segmentation to isolate management-plane systems per AC-4 (Information Flow Enforcement) and CIS 4.4 (Implement and Manage a Firewall on Servers). Conduct a broader review of Cisco management-plane assets in your environment given the documented 2026 exploitation pattern affecting CVE-2026-20128, CVE-2026-20122, and Cisco Unified CM. Review CIS 7.1 (Establish and Maintain a Vulnerability Management Process) to ensure Cisco advisory feeds are included in your vulnerability intake pipeline.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Conduct lessons-learned analysis focused on Catalyst Center management-plane exposure, update detection rules and vulnerability intake processes to cover the broader 2026 Cisco unauthenticated exploit wave (CVE-2026-20128, CVE-2026-20122, Unified CM), and implement durable network segmentation controls.

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Use Shodan or Censys free-tier queries (`product:'Cisco Catalyst Center' port:443`) to audit whether your Catalyst Center instances are indexed as internet-accessible — if they appear in results, they were exposed.

Subscribe to the Cisco PSIRT OpenVuln API (free) and configure a cron job or Python script using `requests` to poll `https://apix.cisco.com/security/advisories/v2/all` daily, filtering on `productName` containing 'Catalyst Center' or 'Cisco DNA Center' and adjacent management-plane products. Build a Sigma rule for path-traversal attempts against Catalyst Center using the patterns identified in Step 2 and publish to your log pipeline to ensure persistent detection beyond this incident.

Evidence: Post-incident documentation artifacts: (1) Full exported access log archive covering the exposure window (from earliest known vulnerable deployment through patch completion), preserved for potential breach notification analysis if sensitive network topology or credentials were accessible via the path traversal. (2) Asset inventory export of all Cisco management-plane systems (Catalyst Center, Unified CM, DNA Center predecessors) with version numbers and network exposure classification, to serve as the baseline for the broader CVE-2026-20128 and CVE-2026-20122 review. (3) Network diagram or firewall rule export documenting pre- and post-incident Catalyst Center network segmentation posture, for lessons-learned record and future audit evidence under NIST AU-11 (Audit Record Retention).

Detection Guidance

Query Catalyst Center web/application access logs for HTTP requests from unauthenticated sessions (no valid session token) that contain path traversal patterns: '../', '..\', URL-encoded variants ('%2e%2e%2f', '%2e%2e%5c'), and double-encoded variants ('%252e%252e%252f'). Focus on requests targeting file system paths outside expected application directories (e.g., '/etc/', '/var/', '/opt/'). Per NIST AU-6 (Audit Record Review, Analysis, and Reporting), establish a regular review cadence for these log sources. Per NIST AU-3 (Content of Audit Records), ensure logs capture source IP, timestamp, full request URI, HTTP method, and response code. Behavioral indicator: repeated 200-series responses to unauthenticated traversal-pattern requests from a single source IP may indicate active file enumeration (T1083) or credential file retrieval (T1552). No specific IOCs (IPs, hashes, domains) were present in the source material for this CVE. MITRE D3FEND countermeasure D3-SFA (System File Analysis) is applicable: monitor system file access patterns for reads of sensitive configuration or credential files originating from the Catalyst Center application process.

Framework Mappings

MITRE-ATTACK

- **T1552** — Unsecured Credentials
- **T1190** — Exploit Public-Facing Application
- **T1083** — File and Directory Discovery

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-3** — Access Enforcement
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **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

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552	Unsecured Credentials	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1
The Hacker News	https://thehackernews.com/2026/06/cisco-unified-cm-flaw-exploited-a...	T2
Computing	https://www.computing.co.uk/news/2026/security/cisco-unified-commun...	T3
Helpnetsecurity	https://www.helpnetsecurity.com/2026/03/05/cisco-cve-2026-20128-cve...	T2
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20191	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1

Generated 2026-07-01 14:59 UTC by TJS Security Command Center