INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 13:48 UTC

Cisco IoT Field Network Director Triple Vulnerability: Command Injection, Path Traversal, and DoS Expose Managed Routers

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0133
Type	CVE Vulnerability
CVE ID	CVE-2026-20167, CVE-2026-20168, CVE-2026-20169
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Cisco IoT Field Network Director (IoT FND), all configurations; releases 4.x and earlier, and 5.x prior to 5.0.0-117
Published	2026-05-06T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Cisco disclosed three vulnerabilities in IoT Field Network Director (IoT FND), a platform used to manage large fleets of industrial and field-deployed routers. The flaws allow a low-privileged attacker to execute commands on managed routers, read restricted files, and disrupt router availability, all remotely, without user interaction. Organizations running IoT FND releases 4.x or earlier, or 5.x prior to 5.0.0-117, should treat patching as a priority given the direct exposure to managed network infrastructure.

Technical Analysis

Cisco disclosed three vulnerabilities in IoT Field Network Director (IoT FND) affecting all deployment configurations. CVE-2026-20167 (CWE-77, CVSS 7.5 per Cisco advisory) is a command injection flaw allowing a low-privileged authenticated remote attacker to execute limited OS commands on managed routers with no user interaction required. CVE-2026-20168 (CWE-22, Path Traversal) enables unauthorized file reads by traversing outside restricted directory boundaries, potentially exposing configuration files or credentials stored on the system. CVE-2026-20169 (CWE-284, Improper Access Control) allows an attacker to trigger denial of service against managed routers. All three are remotely exploitable, require authentication at low privilege level only, and require no user interaction. No workarounds exist. MITRE techniques mapped include T1059 (Command and Scripting Interpreter), T1083 (File and Directory Discovery), T1190 (Exploit Public-Facing Application), T1078.003 (Valid Accounts: Local Accounts), and T1499 (Endpoint Denial of Service). Affected

versions: all 4.x releases and earlier; 5.x releases prior to 5.0.0-117. Fixed version: 5.0.0-117. Source: Cisco PSIRT advisory cisco-sa-iot-fnd-dos-n8N26Q4u.

Action Checklist

1. Step 1: Containment, Identify all IoT FND instances in your environment. Restrict access to the IoT FND management interface to trusted administrative IPs only using network ACLs or firewall rules. Confirm no IoT FND management ports are exposed to the internet or untrusted network segments.
2. Step 2: Detection, Review IoT FND application and access logs for anomalous activity from low-privileged accounts, including unexpected command execution attempts, directory traversal patterns (sequences such as '../' in request paths), and repeated error conditions against managed router endpoints. Correlate against MITRE T1059 and T1083 behavioral patterns in your SIEM.
3. Step 3: Eradication, Upgrade IoT FND to version 5.0.0-117 following the Cisco upgrade path documented in the advisory (cisco-sa-iot-fnd-dos-n8N26Q4u). No configuration-based workaround exists per Cisco PSIRT; patching is the only remediation.
4. Step 4: Recovery, After upgrade, validate that IoT FND version 5.0.0-117 is confirmed in the platform UI and system logs. Verify connectivity and health of all managed routers in the FND inventory. Audit low-privileged IoT FND accounts for any unauthorized changes made prior to patching.
5. Step 5: Post-Incident, Review the access model for IoT FND: low-privileged accounts should not exist for users who do not require read-level access. Implement or tighten role-based access controls within IoT FND. Add IoT FND management traffic to continuous monitoring scope. Evaluate whether managed router configurations were accessed or modified during the exposure window.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal/compliance if IoT FND audit logs confirm that CVE-2026-20167 command injection was exploited to push unauthorized commands to managed routers, or if CVE-2026-20168 path traversal accessed files containing router credentials, encryption keys, or data subject to regulatory protection (e.g., OT/ICS environments with NERC CIP obligations or networks carrying PII/PHI); also escalate if the organization lacks the Cisco software entitlement to download IoT FND 5.0.0-117, as no workaround exists and the environment will remain unremediable without vendor engagement.
Recovery Notes	After upgrading to IoT FND 5.0.0-117, maintain heightened log review of IoT FND access logs and managed router syslog for a minimum of 30 days to detect any attacker persistence mechanisms — such as backdoor accounts, cron jobs, or modified startup configs — that may have been planted on managed routers via CVE-2026-20167 command injection prior to patching. Verify the integrity of router configurations across the entire managed fleet by comparing current running-configs against pre-incident baselines, paying particular attention to AAA configurations, NTP sources, and any changes to SNMP community strings or management ACLs that could indicate an attacker establishing a secondary foothold. Re-run the network ACL and firewall validation from Step 1 after recovery to confirm that management interface restrictions remained in place through the upgrade process and were not inadvertently relaxed.

Forensic Artifacts	IoT FND application access log ('/opt/cgms/server/logs/access.log'): Primary artifact for CVE-2026-20168 path traversal exploitation — contains raw HTTP request URIs; search for encoded traversal sequences ('../', '%2e%2e%2f', '%252e%252e%252f') and file paths outside the IoT FND web root targeting sensitive system or configuration files. | IoT FND audit trail log (admin console: Administration > Audit Trail, or '/opt/cgms/server/logs/cgms.log'): Primary artifact for CVE-2026-20167 command injection — records API-level actions by user account including router command push operations; any OS-level command execution or router configuration change initiated by a low-privileged account is a high-confidence indicator of exploitation. | Managed router running-configuration snapshots and change history in IoT FND inventory: If CVE-2026-20167 was exploited, unauthorized commands may have been pushed to the router fleet — compare current running-configs against last known-good baselines for changes to AAA, ACLs, SNMP, or management interfaces that were not authorized. | IoT FND application server logs (Wildfly/JBoss server.log at '/opt/cgms/server/log/server.log' if applicable): Contains stack traces and error output that may reveal exploitation attempts against CVE-2026-20169 (DoS) including repeated malformed requests or service restart events triggered by the vulnerability. | Network flow or packet capture data for IoT FND management ports (443, 8443) during the exposure window: Source IPs sending repeated requests with traversal patterns or malformed inputs are exploitation indicators; Wireshark capture filter 'tcp.port == 443 && http' on the IoT FND management interface NIC can be used retrospectively if traffic was mirrored, or prospectively to validate that ACL restrictions are effective post-containment.

Per-Action IR Details

Step 1: Containment — Identify all IoT FND instances in your environment. Restrict access to the IoT FND management interface to trusted administrative IPs only using network ACLs or firewall rules. Confirm no IoT FND management ports are exposed to the internet or untrusted network segments.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 12.2 — Establish and Maintain a Secure Network Architecture (IG2/IG3)

Compensating: Without a centralized firewall management platform, enumerate IoT FND instances by querying your asset inventory or running 'nmap -p 443,8443,80,8080 --open -sV' to identify hosts presenting the IoT FND web interface. Apply host-based firewall rules on the IoT FND server immediately: on Linux, run 'iptables -I INPUT -p tcp --dport 443 -j DROP' then 'iptables -I INPUT -p tcp --dport 443 -s -j ACCEPT'. Verify with 'iptables -L -n -v'. Document every IoT FND instance found before making changes — this list becomes your blast radius map.

Evidence: Before restricting access, capture a snapshot of current active TCP sessions to IoT FND management ports (443, 8443) using 'ss -tnp' or 'netstat -anp | grep -E "443|8080"' on the IoT FND host. Export firewall and network ACL rule sets in their pre-change state. Pull IoT FND access logs from the default path '/opt/cgms/server/logs/access.log' (or equivalent for your deployment) to preserve any pre-containment attacker sessions. Capture current authenticated session tokens or active user sessions visible in IoT FND admin console before enforcing IP restrictions.

Step 2: Detection — Review IoT FND application and access logs for anomalous activity from low-privileged accounts, including unexpected command execution attempts, directory traversal patterns (sequences such as '../' in request paths), and repeated error conditions against managed router endpoints. Correlate against MITRE T1059 and T1083 behavioral patterns in your SIEM.

NIST Phase: Detection Analysis

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

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

Compensating: Without a SIEM, grep the IoT FND application log directly for traversal and command injection indicators: 'grep -E "(\.\./|%2e%2e%2f|%252e%252e%252f)" /opt/cgms/server/logs/access.log' for path traversal (CVE-2026-20168) and 'grep -E "(;|\||&&|\`|\$\()" /opt/cgms/server/logs/access.log' for command injection characters (CVE-2026-20167). For DoS indicators tied to CVE-2026-20169, run 'grep -E "(500|503|timeout)" /opt/cgms/server/logs/access.log | awk "{print \$1}" | sort | uniq -c | sort -rn' to identify repeated error-generating source IPs. Deploy a Sigma rule targeting these patterns against syslog forwarding from the IoT FND host if you have a lightweight log aggregator (Graylog, ELK stack free tier).

Evidence: Collect the IoT FND application log ('/opt/cgms/server/logs/cgms.log' and 'access.log'), the IoT FND audit trail log recording API-level actions by user account, and the underlying application server logs (Wildfly/JBoss logs at '/opt/cgms/server/log/server.log' if applicable to your FND deployment). For MITRE T1083 (File and Directory Discovery) indicators from CVE-2026-20168 path traversal exploitation, look for HTTP GET or POST requests containing encoded traversal sequences ('../', '%2e%2e/', '%252e%252e%252f') targeting restricted file paths such as '/etc/passwd', '/opt/cgms/server/conf/', or router credential stores. For T1059 (Command Interpreter) from CVE-2026-20167 command injection, preserve any log entries showing unexpected OS-level command strings (shell metacharacters) appended to API parameters in router management endpoints.

Step 3: Eradication — Upgrade IoT FND to version 5.0.0-117 following the Cisco upgrade path documented in the advisory (cisco-sa-iot-fnd-dos-n8N26Q4u). No configuration-based workaround exists per Cisco PSIRT; patching is the only remediation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), 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: Download IoT FND 5.0.0-117 exclusively from Cisco's official Software Download portal (software.cisco.com) — verify the SHA-512 checksum provided by Cisco against the downloaded package before installation using 'sha512sum '. Follow the documented upgrade path in cisco-sa-iot-fnd-dos-n8N26Q4u; do not attempt a skip-version upgrade without confirming Cisco's supported upgrade matrix, as IoT FND has historically required sequential version steps. Take a full VM snapshot or database backup of the existing IoT FND instance before initiating the upgrade — this is your rollback point if the upgrade fails mid-process.

Evidence: Before patching, capture the current IoT FND version string from the platform UI ('Administration > System Information') and from the CLI or package manager ('rpm -qa | grep cgms' on RHEL-based deployments) for your pre-patch version record. Export the full list of managed router inventory and their last-known configuration hashes from IoT FND so you can detect any router configuration changes that occurred during the exposure window. Preserve pre-upgrade database state including user account audit trails — these are needed for Step 4's account audit and may be overwritten or rotated during upgrade.

Step 4: Recovery — After upgrade, validate that IoT FND version 5.0.0-117 is confirmed in the platform UI and system logs. Verify connectivity and health of all managed routers in the FND inventory. Audit low-privileged IoT FND accounts for any unauthorized changes made prior to patching.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-11 (Audit Record Retention), NIST CM-3 (Configuration Change Control), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Validate version from the CLI in addition to the UI: check 'rpm -qa | grep cgms' or the equivalent installer manifest to confirm 5.0.0-117 is installed and no residual 4.x or earlier 5.x packages remain. For account auditing without a dedicated IAM tool, export the IoT FND user account list via the admin console and cross-reference against your authoritative HR/identity roster; flag any low-privileged accounts that had login activity within the exposure window using 'grep /opt/cgms/server/logs/access.log | grep -E "(POST|PUT|DELETE)"' to identify write-level actions by

accounts that should only have read access. For each managed router showing unexpected configuration changes, pull the router's running-config and compare against the last known-good baseline archived in IoT FND.

Evidence: Post-upgrade, capture the confirmed version string and system log entry recording the upgrade event as your remediation timestamp anchor. Pull IoT FND's built-in audit log for all configuration change events (router pushes, policy modifications, credential changes) executed by low-privileged accounts during the exposure window — this is your primary evidence of whether CVE-2026-20167 command injection was exploited to push unauthorized commands to managed routers. Collect a current configuration snapshot from every managed router in the IoT FND inventory and diff against pre-incident baselines to identify any unauthorized changes that persisted on the routers themselves post-patch.

Step 5: Post-Incident — Review the access model for IoT FND: low-privileged accounts should not exist for users who do not require read-level access. Implement or tighten role-based access controls within IoT FND. Add IoT FND management traffic to continuous monitoring scope. Evaluate whether managed router configurations were accessed or modified during the exposure window.

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 AC-6 (Least Privilege), NIST AU-2 (Event Logging), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For continuous monitoring of IoT FND management traffic without a SIEM, configure syslog forwarding from the IoT FND host to a centralized syslog server (rsyslog or syslog-ng, both free) and write a Sigma rule targeting the traversal and injection patterns identified in Step 2 — run sigma2grep or convert to a cron-scheduled log scan. To enforce least privilege in IoT FND RBAC, audit the built-in role assignments in the IoT FND admin console ('Administration > Users and Roles') and remove operator or admin roles from any account whose function is read-only monitoring; document the role-to-function mapping as your access justification record. Schedule a recurring quarterly access review for IoT FND accounts as a calendar-driven manual control if automated provisioning review is unavailable.

Evidence: For the exposure window assessment, compile the complete HTTP request log from IoT FND covering the period from your earliest vulnerable version deployment through the patch date, and run the traversal and injection grep queries from Step 2 across the full historical log set — not just recent entries. Document whether any managed routers received configuration pushes or credential updates from IoT FND during the exposure window, as CVE-2026-20167 command injection could have been used to propagate unauthorized commands across the entire managed router fleet. Preserve all log evidence, account audit exports, and router configuration diffs in a case-specific evidence folder with write-protected timestamps before closing the incident record.

Detection Guidance

Review IoT FND access and application logs for the following indicators: (1) requests from low-privileged accounts containing path traversal sequences such as '../', '%2e%2e/', or encoded equivalents in file path parameters; (2) unexpected command execution calls or API requests to endpoints that manage router configuration from accounts not associated with administrative roles; (3) elevated error rates or repeated failed requests to managed router endpoints, which may indicate DoS activity via CVE-2026-20169. In your SIEM, correlate IoT FND authentication events (T1078.003) with subsequent file access (T1083) or command invocation (T1059) activity from the same session. No public IOCs or active exploitation indicators are available at this time; detection is behavioral and log-based. EPSS score data is pending NVD publication; limited exploit probability data is available as of this advisory date.

Framework Mappings

MITRE-ATTACK

- **T1083** — File and Directory Discovery
- **T1078.003** — Local Accounts
- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application
- **T1499** — Endpoint Denial of Service

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SC-5** — Denial-of-Service Protection
- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

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

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks

SOC2-TSC

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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery
T1078.003	Local Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1499	Endpoint Denial of Service	Impact

Sources

Source	URL	Tier
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
	https://securityboulevard.com/2026/02/cve-2026-20127-cisco-catalyst...	T3
	https://www.helpnetsecurity.com/2026/03/22/week-in-review-screencon...	T3
	https://blogs.cisco.com/industrial-iot/innovative-ot-security-solut...	T3
Cisco Identity Services Engine Remote Code Execution and Path ...	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20167, CVE-2026-20168, CV...	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1

Generated 2026-05-06 13:48 UTC by TJS Security Command Center