INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-13 16:27 UTC

# Fortinet FortiClient EMS Critical SQL Injection (CVE-2026-21643)

CVE VULNERABILITY | CRITICAL | CVSS 9.8 | CISA KEV

| | |
|---|---|
| SCC Item ID | SCC-CVE-2026-0031 |
| Type | CVE Vulnerability |
| CVE ID | CVE-2026-21643 |
| Severity | CRITICAL |
| CVSS Base Score | 9.8 |
| EPSS Score | 0.1370 (94th percentile) |
| KEV Status | Yes — CISA Known Exploited Vulnerability (due: 2026-04-16) |
| Affected Products | Fortinet FortiClient EMS (confirmed affected version includes 7.4.4; full version range unconfirmed pending NVD detail verification) |
| Published | 2026-04-13 |
| Discovery Source | Cisa Kev |

## Executive Summary

A critical pre-authentication SQL injection vulnerability (CVE-2026-21643, CVSS 9.8) has been confirmed in Fortinet FortiClient EMS, the endpoint management server used to centrally manage enterprise endpoint security clients. An unauthenticated remote attacker can exploit this vulnerability via HTTP requests to execute arbitrary commands on the EMS server, with no credentials required. CISA has confirmed active exploitation in the wild via its Known Exploited Vulnerabilities catalog, indicating real-world attacks are actively occurring.

## Technical Analysis

CVE-2026-21643 is a CWE-89 (Improper Neutralization of Special Elements in SQL Commands) vulnerability in Fortinet FortiClient EMS. Attack vector is network-based, unauthenticated, with no user interaction required, resulting in a CVSS base score of 9.8 (Critical). Confirmed affected version: FortiClient EMS 7.4.4; the full version range across the 7.x branch is unconfirmed pending vendor confirmation. Exploitation is via specially crafted HTTP requests that inject malicious SQL, enabling remote code execution on the EMS server. MITRE ATT&CK techniques mapped: T1190 (Exploit Public-Facing Application) for initial access, T1059 (Command and Scripting Interpreter) for post-exploitation execution. EPSS score is 0.137 at the 94.3rd percentile, indicating the vulnerability ranks in the top 6% of all CVEs by exploitation probability. CISA KEV due date for federal

agencies is 2026-04-16. Full vendor CVSS vector and patched version details are pending verification from the Fortinet PSIRT advisory; consult https://www.fortiguard.com/psirt for the authoritative patch path. NVD record: https://nvd.nist.gov/vuln/detail/CVE-2026-21643.

## Action Checklist

1. Step 1: Containment. Immediately audit your environment for exposed FortiClient EMS instances, specifically version 7.4.4 and any 7.x deployments. If the EMS management interface is internet-facing, restrict access via firewall ACL or network segmentation to trusted management IP ranges only. Restrict access immediately; do not wait for patch availability confirmation. Check Fortinet PSIRT advisory at https://www.fortiguard.com/psirt for any available interim mitigations.
2. Step 2: Detection. Query web/application server logs on the FortiClient EMS host for anomalous HTTP requests containing SQL metacharacters (single quotes, UNION, SELECT, --, ;) in request parameters. Review Windows Event Logs on the EMS host for unexpected process creation events (Event ID 4688) spawned by the EMS service account, which could indicate successful command execution via T1059. Check for new scheduled tasks, service installations, or lateral movement originating from the EMS server. No public IOCs (IPs, hashes, domains) are confirmed at this time.
3. Step 3: Eradication. Apply the official Fortinet patch for CVE-2026-21643 once released via Fortinet PSIRT. Verify the specific patched version number from the Fortinet advisory before upgrading, as the full affected version range is not yet confirmed in NVD. If the system shows signs of compromise, treat it as a full incident: isolate, forensically preserve, and rebuild from clean media rather than patch in place.
4. Step 4: Recovery. After patching, verify the EMS service is running the patched build and re-run a vulnerability scan against the management interface to confirm the injection endpoint no longer accepts crafted payloads. Monitor the EMS server for 30 days post-remediation for signs of persistence mechanisms installed prior to patching (scheduled tasks, new local accounts, unexpected outbound connections). Re-enable external access only after access control restrictions are validated.
5. Step 5: Post-Incident. Audit your internet-facing application inventory and confirm all administrative management interfaces (not just Fortinet) are restricted to management networks. If exploitation is confirmed, initiate forensic review of EMS-connected endpoints for signs of lateral movement. Review your patch SLA process: CISA KEV items require federal agencies to patch by 2026-04-16; align your internal SLA accordingly. Evaluate whether a WAF or IPS rule for SQL injection signatures was in the traffic path for this service.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to CISO and legal/privacy counsel immediately if Windows Event ID 4688 or Sysmon Event ID 1 confirms cmd.exe, powershell.exe, or any non-EMS process spawned by the EMS service account, OR if Event ID 4624 logon events show lateral movement from the EMS server to any other internal host, as this indicates confirmed RCE and potential breach of all EMS-managed endpoints, which may trigger regulatory notification obligations depending on the data processed by or accessible to the EMS server. |

| | |
|---|---|
| **Recovery Notes** | After patching to the Fortinet-confirmed fixed build, validate remediation by confirming `xp_cmdshell` is disabled in MS SQL Server (`EXEC sp_configure 'xp_cmdshell'; -- expected value_in_use: 0`) and re-running a controlled SQL injection probe against the EMS management endpoint from an internal test host to verify the patched build rejects malformed input. Monitor the EMS host and all EMS-managed endpoints for 30 days post-patch using Sysmon Event ID 1 (process creation) and Event ID 3 (network connection) filtered on the EMS service account and EMS server IP respectively, as pre-patch persistence mechanisms (scheduled tasks, implanted services, rogue SQL logins) may activate after the patch window. Do not restore external access to the EMS management interface until network segmentation controls have been validated by a second reviewer and documented. |
| **Forensic Artifacts** | IIS/EMS web server access logs at C:\inetpub\logs\LogFiles\W3SVC\ containing HTTP requests with URI-encoded SQL metacharacters (%27, UNION, SELECT, xp_cmdshell) directed at EMS management endpoints — the primary artifact of SQL injection exploitation attempts against CVE-2026-21643 \| MS SQL Server ERRORLOG at C:\Program Files\Microsoft SQL Server\MSSQL\MSSQL\Log\ERRORLOG and transaction log backup showing injected SQL statements processed by the EMS backend database, including any xp_cmdshell invocations that indicate successful escalation from injection to OS command execution \| Windows Security Event Log Event ID 4688 (Process Creation) on the EMS host filtered for cmd.exe, powershell.exe, wscript.exe, or mshta.exe spawned as child processes of the FortiClient EMS service process — the direct artifact of successful RCE via MITRE T1059 following SQL injection exploitation \| Windows Task Scheduler Operational Log (Microsoft-Windows-TaskScheduler/Operational) and registry key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks for scheduled tasks created during the exploitation window — attacker-installed persistence mechanism following RCE on the EMS server \| FortiClient endpoint agent push logs on EMS-managed endpoints documenting any unauthorized configuration changes, policy modifications, or software deployments issued from the compromised EMS server during the exploitation window — critical for determining whether the EMS server was weaponized to push malicious content to managed endpoints enterprise-wide |

### Per-Action IR Details

**Step 1: Containment — Immediately audit your environment for exposed FortiClient EMS instances, specifically version 7.4.4 and any 7.x deployments. If the EMS management interface is internet-facing, restrict access via firewall ACL or network segmentation to trusted management IP ranges only. Do not wait for patch confirmation before restricting exposure. Check Fortinet PSIRT advisory at https://www.fortiguard.com/psirt for any available interim mitigations.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy (CSF RS function): isolate affected systems and restrict attack surface before eradication is possible

**Controls:** NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

**Compensating:** On the EMS host or upstream perimeter, run: `netsh advfirewall firewall add rule name='Block EMS External' dir=in action=block remoteip=any localip= localport= protocol=TCP` to block all non-management IPs. On Linux/network firewall: `iptables -I INPUT -p tcp --dport -j DROP` followed by explicit ACCEPT rules for trusted management CIDR blocks. Enumerate FortiClient EMS hosts using osquery: `SELECT * FROM listening_ports WHERE port=;` to confirm exposure scope. Use `nmap -sV -p ` from an internal scanner to identify any additional unmanaged EMS instances running version 7.x.

**Evidence:** Before making any ACL changes, capture the current network exposure state: run `netstat -ano` on the EMS Windows host and record all established and listening connections on the EMS management port. Export the

Windows Firewall effective policy via `netsh advfirewall export C:\fw_snapshot_pre_containment.wfw`. Pull IIS or EMS application access logs (default path: `C:\Program Files\Fortinet\FortiClient EMS\logs\` and IIS logs at `C:\inetpub\logs\LogFiles\`) covering the 30 days prior to containment to preserve pre-isolation evidence of inbound HTTP requests. Record all source IPs that have reached the EMS interface — these are candidate attacker IPs for later correlation.

**Step 2: Detection — Query web/application server logs on the FortiClient EMS host for anomalous HTTP requests containing SQL metacharacters (single quotes, UNION, SELECT, --, ;) in request parameters. Review Windows Event Logs on the EMS host for unexpected process creation events (Event ID 4688) spawned by the EMS service account, which could indicate successful command execution via T1059. Check for new scheduled tasks, service installations, or lateral movement originating from the EMS server. No public IOCs (IPs, hashes, domains) are confirmed at this time.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis (CSF DE function): correlate log sources to determine scope of exploitation, distinguish reconnaissance from confirmed RCE, and classify the incident

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

**Compensating:** Enable Process Creation Auditing on the EMS host if not already active: `auditpol /set /subcategory:'Process Creation' /success:enable /failure:enable`. Deploy Sysmon with a community config (SwiftOnSecurity or Olaf Hartong) targeting the EMS service account; key Sysmon Event IDs for this threat: Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create). Query Windows Security Event Log for EMS-specific process spawning with PowerShell: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'fctems|FortiClientEMS'}`. For SQL injection pattern detection without a SIEM, parse IIS/EMS logs with: `Select-String -Path 'C:\inetpub\logs\LogFiles\*\*.log' -Pattern '"|UNION|SELECT|--|;|xp_cmdshell|EXEC\s*\(" -CaseSensitive:$false | Export-Csv sqli_hits.csv`. Use Sigma rule `proc_creation_win_susp_cmd_spawn_from_web_server.yml` (available in SigmaHQ repository) adapted to match the FortiClient EMS service account name as the parent process.

**Evidence:** Collect the following BEFORE log rotation or system changes: (1) IIS access logs at `C:\inetpub\logs\LogFiles\W3SVC\` — look for POST/GET requests with URI-encoded SQL metacharacters (`%27`, `%3B`, `%2D%2D`, `UNION`, `SELECT`, `xp_cmdshell`) in parameters handled by the EMS web endpoint. (2) Windows Security Event Log (Event ID 4688) filtered on processes spawned by the FortiClient EMS service account (typically running as SYSTEM or a dedicated service account) — cmd.exe, powershell.exe, or wscript.exe as child processes of the EMS process indicate successful RCE via MITRE T1059. (3) Windows System Event Log for new service installations (Event ID 7045) or Task Scheduler logs (`Microsoft-Windows-TaskScheduler/Operational`) for tasks created in the exploitation window. (4) FortiClient EMS application logs at `C:\Program Files\Fortinet\FortiClient EMS\logs\` for database error messages or unusual query patterns that indicate injected SQL was processed by the backend database (typically MS SQL Server — check SQL Server ERRORLOG at `C:\Program Files\Microsoft SQL Server\MSSQL\MSSQL\Log\ERRORLOG`). (5) Network flow logs or firewall logs showing outbound connections from the EMS server to external IPs — successful RCE may produce reverse shell or C2 beacon traffic.

**Step 3: Eradication — Apply the official Fortinet patch for CVE-2026-21643 once released via Fortinet PSIRT. Verify the specific patched version number from the Fortinet advisory before upgrading — the full affected version range is not yet confirmed in NVD. If the system shows signs of compromise, treat it as a full incident: isolate, forensically preserve, and rebuild from clean media rather than patch in place.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication (CSF RS function): remove the threat from the environment and verify the vulnerability has been remediated; if compromise is confirmed, rebuild rather than remediate in place

**Controls:** NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

**Compensating:** Before patching, capture a full forensic image of the EMS host using a free tool such as `FTK Imager Lite` (portable, no install required) or `dd` via a bootable Linux USB to preserve evidence of pre-patch state. Verify patch integrity after download by comparing the SHA-256 hash of the Fortinet update package against the hash published in the Fortinet PSIRT advisory: `Get-FileHash -Algorithm SHA256 `. If rebuilding from clean media, use Fortinet's documented EMS backup/restore procedure to restore the endpoint client database after confirming the backup predates the exploitation window — do not restore a backup that may contain attacker-planted persistence. Post-install, run `Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -match 'FortiClient EMS'}` to confirm the installed version matches the patched build number from the advisory.

**Evidence:** Forensic preservation required BEFORE eradication: (1) Take a full memory image of the EMS server using `WinPmem` (free, open-source) to capture any in-memory payloads, injected shellcode, or active attacker sessions that will not survive a reboot or patch — this is critical if Event ID 4688 or Sysmon Event ID 1 showed suspicious child processes of the EMS service. (2) Export the MS SQL Server database transaction log (`BACKUP LOG [EMS_DB] TO DISK='C:\forensics\ems_txlog.bak' WITH FORMAT`) to preserve a record of injected SQL statements processed by the EMS backend. (3) Run `reg export HKLM\SYSTEM\CurrentControlSet\Services C:\forensics\services_pre_patch.reg` and `schtasks /query /fo CSV /v > C:\forensics\tasks_pre_patch.csv` to document service and scheduled task state prior to any changes — attacker persistence installed via RCE will appear here. (4) Collect the full EMS application directory `C:\Program Files\Fortinet\FortiClient EMS\` using robocopy or tar to preserve any web shells or dropped binaries placed by the attacker via command execution.

**Step 4: Recovery — After patching, verify the EMS service is running the patched build and re-run a vulnerability scan against the management interface to confirm the injection endpoint no longer accepts crafted payloads. Monitor the EMS server for 30 days post-remediation for signs of persistence mechanisms installed prior to patching (scheduled tasks, new local accounts, unexpected outbound connections). Re-enable external access only after access control restrictions are validated.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery (CSF RC function): restore systems to normal operation, verify integrity of the remediated environment, and confirm no attacker persistence survives the patch

**Controls:** NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

**Compensating:** Perform post-patch validation without a commercial scanner using `sqlmap` (open-source) in safe/non-destructive mode against your own EMS instance from an internal test host: `sqlmap -u 'https://:/' --level=1 --risk=1 --batch` — confirm the injection point returns no exploitable result with the patched build. Enumerate all local accounts created after the estimated exploitation window: `net user` and cross-reference against your baseline; investigate any account not in your asset inventory. Monitor outbound connections from the EMS server using `netstat -ano` in a scheduled task every 15 minutes logging to a file, or deploy Sysmon Event ID 3 (Network Connection) filtering on connections initiated by EMS service processes to detect C2 beaconing from pre-patch implants. Use `Get-ScheduledTask | Where-Object {$_.Date -gt ''}` to surface tasks created during the exposure window.

**Evidence:** Before re-enabling any external access: (1) Run a diff of current scheduled tasks and services against the pre-patch snapshots captured during eradication to identify any persistence that survived patching. (2) Query Windows Security Event Log for Event ID 4720 (local account created) and Event ID 4732 (account added to privileged group) with timestamps in the exploitation window — attacker account creation via RCE is a primary persistence technique following SQL injection to RCE on Windows. (3) Check MS SQL Server for new SQL logins or `xp_cmdshell` enablement: `SELECT name, type_desc, create_date FROM sys.server_principals WHERE create_date > ''` and `SELECT value_in_use FROM sys.configurations WHERE name = 'xp_cmdshell'` — this specific vulnerability's RCE path likely involves `xp_cmdshell` or equivalent SQL Server command execution, so its enabled state is a direct indicator of attacker activity.

**Step 5: Post-Incident — Audit your internet-facing application inventory and confirm all administrative management interfaces (not just Fortinet) are restricted to management networks. If exploitation is confirmed, initiate forensic review of EMS-connected endpoints for signs of lateral movement. Review your patch SLA process: CISA KEV items require federal agencies to patch by 2026-04-16; align your internal SLA**

**accordingly. Evaluate whether a WAF or IPS rule for SQL injection signatures was in the traffic path for this service.**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity (CSF GV/ID functions): lessons learned, detection gap analysis, policy updates, and intelligence sharing to prevent recurrence

**Controls:** NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** For lateral movement forensics on EMS-connected endpoints without EDR: deploy osquery on endpoints using `osquery`'s `process_open_sockets`, `logged_in_users`, and `shell_history` tables to identify anomalous activity originating from the EMS server's IP during the exploitation window. Use a free Sigma rule pack (SigmaHQ `windows/lateral_movement/`) converted to Windows Event Log queries via `sigmac` to hunt for pass-the-hash, PsExec, or WMI lateral movement sourced from the EMS server. For WAF gap analysis without budget: deploy `ModSecurity` (open-source WAF) with the OWASP Core Rule Set (CRS) in front of the EMS management interface — CRS rules 942100–942999 cover SQL injection detection and would have provided a detection layer for CVE-2026-21643 injection patterns. Document the gap formally in your risk register.

**Evidence:** Post-incident forensic scope for EMS-connected endpoints: (1) On Windows endpoints managed by the compromised EMS instance, query Windows Security Event Log for Event ID 4624 (logon) with Logon Type 3 (network) or Type 10 (remote interactive) sourced from the EMS server IP during the exploitation window — these indicate the attacker used the EMS server as a pivot point. (2) Review FortiClient endpoint agent logs on managed endpoints for unauthorized policy changes, configuration pushes, or software deployments issued from the EMS server during the suspected compromise window — the EMS server has the authority to push configuration and potentially executables to all managed endpoints, making it a high-value pivot. (3) Collect DNS query logs from endpoints for resolution of external domains during the exploitation window — if the attacker achieved RCE on EMS and pivoted, beaconing from endpoint agents or the EMS server itself would appear as anomalous external DNS queries.

## Detection Guidance

Primary detection focus is the FortiClient EMS web application layer. Review IIS or embedded web server logs on the EMS host for HTTP requests containing SQL injection patterns in URI parameters or POST body data: look for single quotes, double dashes, UNION SELECT sequences, encoded variants (%27, %2D%2D), and abnormally long parameter strings. On Windows, monitor Event ID 4688 (process creation) filtered to the EMS service account as parent process; unexpected child processes (cmd.exe, powershell.exe, wscript.exe) are a high-confidence indicator of successful exploitation. Enable PowerShell Script Block Logging (Event ID 4104) on the EMS host if not already active. Check for new local administrator accounts (Event ID 4720, 4732) and new scheduled tasks (Event ID 4698). Network-level: alert on outbound connections from the EMS server to external IPs, particularly over non-standard ports, which may indicate C2 activity post-exploitation. Establish baseline EMS server behavior (typical process, network, and log patterns) before anomalies occur. Any deviation from baseline, unexpected child processes, new user accounts, outbound connections to unknown IPs, should trigger incident response escalation.

## Framework Mappings

### MITRE-ATTACK

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

### 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
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

### OWASP-TOP10-2021

- **A03:2021** — Injection

### CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications

### ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities

### HIPAA-SECURITY

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

### SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

### 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 |
|---|---|---|
| T1059 | Command and Scripting Interpreter | Execution |
| T1190 | Exploit Public-Facing Application | Initial-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| **cisa_kev** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog | T1 |
| **CVE-2026-21643 Detail - NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-21643 | T1 |
| **CVE-2026-21643: Critical SQL Injection in FortiClientEMS** | https://arcticwolf.com/resources/blog/cve-2026-21643/ | T3 |
| **Pre-Authentication SQL Injection in FortiClient EMS 7.4.4** | https://bishopfox.com/blog/cve-2026-21643-pre-authentication-sql-in... | T3 |
| **CVE-2026-21643 : An improper neutralization of special ...** | https://www.cvedetails.com/cve/CVE-2026-21643/ | T3 |