INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 14:15 UTC

Schneider Electric OT Products Affected by Session Hijacking Flaw (CVE-2026-4827) Across 30+ Critical Infrastructure Devices

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0324
Type	CVE Vulnerability
CVE ID	CVE-2026-4827
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0031 (23th percentile)
Affected Products	Schneider Electric Easergy MiCOM series (C264, P138, P139, P436-P439, P532, P539, P631-P634, P638, C434, P40 Series), EcoStruxure Power Automation System Gateway (EPAS-GTW), EcoStruxure Power Automation System UI (EPAS-UI), EcoStruxure Power Operation (2022/2024), iPMFLS, PowerLogic P5, PowerLogic P7, PowerLogic T300, PowerLogic T500, Easergy C5, Saitel DP, EasyLogic T150 (Saitel DR)
Published	2026-06-18T12:00:00+00:00
Discovery Source	Rss:T2 Gov

Executive Summary

A session hijacking vulnerability in Schneider Electric's OT product portfolio allows network-adjacent attackers to predict or brute-force session tokens and take over authenticated sessions without credentials. More than 30 product lines are affected, including protection relays, power automation gateways, and energy management platforms used across energy, water, critical manufacturing, and chemical sectors worldwide. Organizations running unpatched Schneider Electric Easergy MiCOM, EcoStruxure, PowerLogic, or related systems face risk of unauthorized control-plane access that could disrupt or manipulate industrial operations.

Technical Analysis

CVE-2026-4827 is a CWE-331 (Insufficient Entropy) flaw disclosed via CISA advisory ICSA-26-169-07, affecting Schneider Electric Easergy MiCOM series (C264, P138, P139, P436-P439, P532, P539, P631-P634, P638, C434, P40 Series), EcoStruxure Power Automation System Gateway (EPAS-GTW), EcoStruxure Power Automation System UI (EPAS-UI), EcoStruxure Power Operation (2022 and 2024), iPMFLS, PowerLogic P5,

P7, T300, T500, Easergy C5, Saitel DP, and EasyLogic T150 (Saitel DR). Associated weaknesses CWE-330 (Use of Insufficiently Random Values) and CWE-384 (Session Fixation) indicate a systemic design deficiency in session management across the product family, not an isolated coding error. Attack vector is network-adjacent with no authentication required (CVSS base 7.5 per NVD). MITRE ATT&CK ICS techniques mapped include T1563 (Remote Service Session Hijacking), T1078 (Valid Accounts), T1040 (Network Sniffing), T0869 (Standard Application Layer Protocol), T0861 (Point-to-Point Communication), and T0855 (Unauthorized Command Message). Patches are available for most product lines; several MiCOM P30 series models remain unpatched, with vendor-issued mitigations as the only available defense. Operators should consult ICSA-26-169-07 directly for per-product patch availability and version-specific guidance.

Action Checklist

1. Step 1: Containment, Immediately audit network segmentation for all affected Schneider Electric devices listed in ICSA-26-169-07. Restrict network-adjacent access to affected devices by enforcing strict firewall rules and VLAN isolation. Where network-adjacent access cannot be restricted, prioritize those devices for emergency patching. Reference: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Review session logs on EcoStruxure Power Operation, EPAS-GTW, EPAS-UI, and PowerLogic management interfaces for anomalous session establishment events, particularly sessions initiated without a preceding authentication event or from unexpected source IPs. Monitor for repeated session token requests from a single host (indicative of brute-force token prediction). Enable network traffic capture on OT segments to detect T1040 (network sniffing) activity. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, Apply all available patches per Schneider Electric's guidance referenced in ICSA-26-169-07. For MiCOM P30 series models without available patches, implement vendor-recommended mitigations (network isolation, disable unused remote access services) and document the exception. Rotate all session credentials and force re-authentication across affected systems post-patch. Reference: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), and D3-CRO (Credential Rotation).
4. Step 4: Recovery, After patching, validate that session token generation meets entropy requirements by reviewing vendor release notes for the specific fix. Re-enable remote management interfaces only after patching is confirmed. Monitor affected systems for 30 days post-remediation for anomalous session activity. Reference: NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), D3-LAM (Local Account Monitoring).
5. Step 5: Post-Incident, Conduct a control gap review against NIST AC-17 (Remote Access) and AC-2 (Account Management) to assess whether OT session management policies require formal documentation and testing. Evaluate whether current OT network architecture enforces least-privilege access per NIST AC-6 (Least Privilege). Add Schneider Electric OT product patching to your vulnerability management cadence per CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and CIS 7.2 (Establish and Maintain a Remediation Process). Apply D3-MFA (Multi-factor Authentication) where supported on affected management interfaces.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and OT security management if any Easergy MiCOM protection relay, EcoStruxure Power Operation node, or PowerLogic device shows evidence of an authenticated session established without a correlated login event, or if anomalous control commands (e.g., relay trips, breaker operations, load shedding) are observed on affected devices during the investigation window, as this indicates active session hijack exploitation with potential physical consequence in energy, water, or critical manufacturing environments.
Recovery Notes	After patching, confirm session token entropy improvement by reviewing Schneider Electric's ICSA-26-169-07 patch release notes for explicit mention of the token generation algorithm change and validate that no legacy firmware versions remain in inventory across all 30+ affected product lines. Re-enable remote management interfaces (HTTP/HTTPS on Easergy MiCOM, IEC 61850 MMS on PowerLogic P5/P7, and EcoStruxure API endpoints) strictly in sequence — only after per-device patch confirmation — and verify each interface requires fresh authentication. Maintain elevated monitoring (daily log review using the syslog aggregation or Wireshark procedures established in Steps 2 and 4) for a minimum of 30 days post-remediation given the network-adjacent attack vector and the breadth of affected critical infrastructure sectors.
Forensic Artifacts	EcoStruxure Power Operation and EPAS-UI application session logs (default: %ProgramData%\Schneider Electric\EcoStruxure Power Operation\logs\) — look for session_start or token_issued events with no correlated authentication POST from the same source IP within the preceding 60 seconds, which is the primary forensic indicator of token prediction or brute-force exploitation specific to CVE-2026-4827. | Network packet capture (pcap) from the OT segment mirror port filtered on TCP port 443/80 and IEC 61850 MMS port 102 — examine for high-frequency session establishment attempts from a single MAC/IP address targeting Easergy MiCOM management interfaces, consistent with the network-adjacent brute-force token prediction attack vector described in the advisory. | Easergy MiCOM relay internal event logs exported via device CLI or vendor management tool (IEC 61850 GOOSE/MMS log records) — anomalous operator command events (relay configuration changes, protection setting modifications, or control output activations) logged under a session ID that has no corresponding authentication event are direct evidence of session hijack exploitation reaching the operational layer. | Windows Security Event Log on EPAS-GTW and EPAS-UI hosts — Event ID 4624 (Logon) and Event ID 4776 (Credential Validation) records should be correlated against application-layer session tokens; a session token active in the application log with no matching 4624 event in the OS log within the session window indicates a hijacked session bypassing OS-layer authentication. | PowerLogic P5/P7/T300/T500 and Saitel DP web interface access logs (retrievable via device TFTP export or serial console) — filter for HTTP GET/POST requests to session management endpoints (typically /api/session or /cgi-bin/session) from source IPs not present in the approved engineering workstation inventory, which would indicate unauthorized network-adjacent access exploiting the predictable session token flaw.

Per-Action IR Details

Step 1: Containment — Immediately audit network segmentation for all affected Schneider Electric devices listed in ICSA-26-169-07. Restrict network-adjacent access to affected devices by enforcing strict firewall rules and VLAN isolation. Where network-adjacent access cannot be restricted, prioritize those devices for emergency patching. Reference: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

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

Compensating: For teams without NAC or enterprise firewall management: apply host-based ACLs on the engineering workstation or historian that communicates with Easergy MiCOM and EcoStruxure devices using Windows Firewall with Advanced Security (netsh advfirewall) or iptables on Linux jump hosts to restrict inbound connections to the device management ports (typically TCP 80/443/102 for IEC 61850 MMS and Modbus TCP 502). Use Wireshark on the OT segment switch mirror port to confirm no lateral traffic is reaching affected VLAN segments from untrusted subnets.

Evidence: Before enforcing new firewall rules or reconfiguring VLANs, capture a full packet capture (pcap) of current network-adjacent traffic to affected devices using Wireshark or tcpdump on the OT segment mirror port — preserving any in-progress session hijack attempts. Record active ARP tables (`arp -a`) on engineering workstations and historians that communicate with Easergy MiCOM (C264, P138, P139, P436–P439, P532, P539, P631–P634, P638, C434, P40 series) and EcoStruxure Power Operation nodes to document currently active neighbors before VLAN changes break adjacency. Also capture active TCP connection state (`netstat -ano` or `Get-NetTCPConnection`) on any Windows-based EPAS-GTW or EPAS-UI hosts before isolation.

Step 2: Detection — Review session logs on EcoStruxure Power Operation, EPAS-GTW, EPAS-UI, and PowerLogic management interfaces for anomalous session establishment events, particularly sessions initiated without a preceding authentication event or from unexpected source IPs. Monitor for repeated session token requests from a single host (indicative of brute-force token prediction). Enable network traffic capture on OT segments to detect T1040 (network sniffing) activity. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

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-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell on the EcoStruxure Power Operation and EPAS-UI Windows hosts to parse IIS or application session logs for HTTP 200 responses on session establishment endpoints where no prior POST to the authentication endpoint appears within the same source IP session window: `Select-String -Path 'C:\ProgramData\Schneider Electric\...\logs\*.log' -Pattern 'session|token|auth'`. On Linux-based EPAS-GTW nodes, run `grep -E 'session|token|login' /var/log/epas/*.log | awk '{print $1,$2,$NF}' | sort | uniq -c | sort -rn` to surface high-frequency session token requests from a single source. Deploy a Sigma rule targeting HTTP session creation events without a correlated authentication event in the preceding 30-second window on the same source IP.

Evidence: Collect EcoStruxure Power Operation application session logs (default path varies by version; typically under `%ProgramData%\Schneider Electric\EcoStruxure Power Operation\logs\`) and EPAS-GTW syslog output before any session invalidation or service restart. Capture live TCP sessions on management interface ports (TCP 443/80) using `netstat -ano` or `ss -tnp` to identify source IPs with anomalously high session establishment rates indicative of token brute-force. Preserve PowerLogic P5/P7/T300/T500 and Saitel DP web interface access logs from the device's internal logging (accessible via device CLI or TFTP export) before any patch application that may rotate or truncate log storage.

Step 3: Eradication — Apply all available patches per Schneider Electric's guidance referenced in ICSA-26-169-07. For MiCOM P30 series models without available patches, implement vendor-recommended mitigations (network isolation, disable unused remote access services) and document the exception. Rotate all session credentials and force re-authentication across affected systems post-patch. Reference: NIST SI-4 is not mapped in the knowledge base for this specific step; apply CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management), and D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For OT environments where automated patch management tooling is absent or prohibited: manually download firmware updates for each affected Easergy MiCOM model (C264, P138, P139, P436–P439, P532, P539, P631–P634, P638, C434, P40 series) and EcoStruxure Power Operation 2022/2024 directly from Schneider Electric's Asset Centre portal, verify SHA-256 checksums against ICSA-26-169-07 advisory values before flashing, and maintain a signed change record. For MiCOM P30 series devices pending patch availability, disable the HTTP/HTTPS management interface via device CLI (`set webserver disable`) and remove device management access from all non-engineering VLANs using the compensating firewall rules established in Step 1.

Evidence: Before applying any firmware or software patch to Easergy MiCOM relays or EcoStruxure nodes — which will alter or erase volatile device state — capture: (1) a full export of the device's current session table or active connection list via device CLI or vendor management tool; (2) a memory acquisition of Windows-based EPAS-GTW and EPAS-UI hosts using WinPmem or Magnet RAM Capture to preserve in-memory session token values and any injected or anomalous process artifacts; (3) a pre-patch snapshot of EcoStruxure Power Operation event logs and PowerLogic T300/T500 audit trails exported to a forensic hold location, since patching may reset or overwrite internal log buffers on embedded devices.

Step 4: Recovery — After patching, validate that session token generation meets entropy requirements by reviewing vendor release notes for the specific fix. Re-enable remote management interfaces only after patching is confirmed. Monitor affected systems for 30 days post-remediation for anomalous session activity. Reference: NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), D3-LAM (Local Account Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without an enterprise monitoring platform: configure syslog forwarding from EcoStruxure Power Operation and EPAS-GTW to a centralized syslog receiver (syslog-ng or rsyslog on a dedicated Linux VM) and write a daily cron job that runs `grep -c 'session_start\|auth_bypass\|token_request' /var/log/remote/schneider-*.log` and emails a count summary to the IR team. For Easergy MiCOM relays accessible via IEC 61850 MMS, use Wireshark with a capture filter (`tcp port 102`) on the OT segment mirror port for the first 30 days post-patch to detect any residual unauthorized session establishment attempts against the protection relay management interfaces.

Evidence: Before re-enabling any remote management interfaces on PowerLogic P5, P7, T300, T500, Easergy C5, Saitel DP, or EasyLogic T150 devices, document the current interface state (enabled/disabled status, bound IP, active sessions) via device CLI output or vendor management console screenshot as a recovery baseline. This preserves a clean post-eradication state record for post-incident review and confirms no active sessions survive from the pre-patch compromise window.

Step 5: Post-Incident — Conduct a control gap review against NIST AC-17 (Remote Access) and AC-2 (Account Management) to assess whether OT session management policies require formal documentation and testing. Evaluate whether current OT network architecture enforces least-privilege access per NIST AC-6 (Least Privilege). Add Schneider Electric OT product patching to your vulnerability management cadence per CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and CIS 7.2 (Establish and Maintain a Remediation Process). Apply D3-MFA (Multi-factor Authentication) where supported on affected management interfaces.

NIST Phase: Post Incident

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

Controls: NIST AC-17 (Remote Access), NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation

Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams lacking a formal GRC platform: create a spreadsheet-based control gap register that maps each affected Schneider Electric product line (Easergy MiCOM series, EcoStruxure Power Operation 2022/2024, PowerLogic P5/P7/T300/T500, Saitel DP, EasyLogic T150) against AC-17 remote access policy documentation status, AC-6 least-privilege role assignments, and MFA support per vendor release notes. Schedule a quarterly review cadence tied to Schneider Electric's PSIRT advisory feed (subscribe at https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp — recommend human validation of current URL) to ensure CVE-2026-4827-class session management vulnerabilities across this product family are caught proactively in future patch cycles.

Evidence: No volatile evidence capture is required for this post-incident phase. Assemble the forensic hold package from prior steps — pre-patch session logs, memory acquisitions from EPAS-GTW/EPAS-UI hosts, pcap files from the OT segment, and device CLI session table exports — and archive them per your organization's incident record retention policy (NIST AU-11 Audit Record Retention) before closing the incident. This package supports lessons-learned analysis and any regulatory notification requirements under NERC CIP or ICS-CERT reporting obligations applicable to energy and critical manufacturing sector operators affected by this vulnerability.

Detection Guidance

Focus detection on session management anomalies across affected Schneider Electric management interfaces. Key indicators: (1) Session establishment events with no preceding authentication record in the same log source, suggests session token prediction or fixation. (2) Repeated session initiation attempts from a single source IP within short time windows against EPAS-GTW, EPAS-UI, or EcoStruxure Power Operation web interfaces, consistent with token brute-force. (3) Network captures showing sequential or low-entropy session token values in HTTP/application layer traffic on OT segments (MITRE T1040, T0869). (4) Authenticated sessions originating from IPs outside expected engineering workstation ranges, particularly in environments where remote access is tightly controlled. Log sources to prioritize: application logs from EcoStruxure Power Operation and EPAS-UI, firewall/IDS logs on OT network segments, and any available session audit logs from MiCOM relay management interfaces. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs). D3FEND countermeasures: D3-LAM (Local Account Monitoring), D3-SFA (System File Analysis) for session configuration files.

Framework Mappings

MITRE-ATTACK

- **T0869** — Standard Application Layer Protocol
- **T1078** — Valid Accounts
- **T1563** — Remote Service Session Hijacking
- **T0861** — Point & Tag Identification
- **T0855** — Unauthorized Command Message
- **T0865** — Spearphishing Attachment
- **T1040** — Network Sniffing

NIST-800-53R5

- **AC-2** — Account Management

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

CIS-V8

- **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

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

SOC2-TSC

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T0869	Standard Application Layer Protocol	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1563	Remote Service Session Hijacking	Lateral-Movement
T0861	Point & Tag Identification	Collection
T0855	Unauthorized Command Message	Impair-Process-Control
T0865	Spearphishing Attachment	Initial-Access
T1040	Network Sniffing	Credential-Access

Sources

Source	URL	Tier
ICS Advisories	https://www.cisa.gov/news-events/ics-advisories/icsa-26-169-07	T1
CVE-2026-4827 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-4827	T1

Source	URL	Tier
CVE-2026-4827: Insufficient Entropy Auth Bypass Flaw - SentinelOne	https://www.sentinelone.com/vulnerability-database/cve-2026-4827/	T3
CVE-2026-4827 | Tenable®	https://www.tenable.com/cve/CVE-2026-4827	T3
CVE-2026-4827 - CVE Details, Severity, and Analysis | Strobes VI	https://vi.strobes.co/cve/CVE-2026-4827	T3