INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-09 19:32 UTC

# Schneider Electric EcoStruxure Panel Server Credential Reset Flaw Exposes OT Gateways in Critical Infrastructure

CVE VULNERABILITY | HIGH | CVSS 7.5

| | |
|---|---|
| SCC Item ID | SCC-CVE-2026-0282 |
| Type | CVE Vulnerability |
| CVE ID | CVE-2026-6866 |
| Severity | HIGH |
| CVSS Base Score | 7.5 |
| EPSS Score | 0.0006 (20th percentile) |
| Affected Products | Schneider Electric EcoStruxure Panel Server PAS800, PAS800V2, PAS600, PAS600V2, PAS400, firmware versions 002.005.000 and prior; PAS800, PAS800V2, PAS600, PAS600V2, PAS400 on 002.006.000 also noted as affected in source data |
| Published | 2026-06-09T12:00:00+00:00 |
| Discovery Source | Rss:T2 Gov |

## Executive Summary

A firmware flaw in Schneider Electric EcoStruxure Panel Server devices can cause credentials to silently revert to factory defaults, allowing unauthorized access to OT gateways that bridge industrial control networks to cloud applications. Affected models (PAS400, PAS600, PAS600V2, PAS800, PAS800V2) running firmware 002.005.000 or earlier are exposed; Schneider Electric has released firmware 002.006.000 as the fix. Organizations operating these devices in critical infrastructure environments, including energy, utilities, and manufacturing, face risk of unauthorized OT network access if the flaw triggers under the undisclosed rare conditions.

## Technical Analysis

CVE-2026-6866 (CVSS 3.1: 7.5, HIGH) affects Schneider Electric EcoStruxure Panel Server models PAS400, PAS600, PAS600V2, PAS800, and PAS800V2 running firmware 002.005.000 and prior. Under unspecified rare conditions, the device credential state reverts to factory defaults, enabling authentication bypass without valid credentials. The vulnerability is classified under CWE-1188 (Insecure Default Initialization of Resource), CWE-255 (Credentials Management Errors), and CWE-287 (Improper Authentication). The Panel Server acts as a cloud-connected IoT/OT gateway, meaning successful exploitation could expose downstream OT assets to

unauthorized command or data access. Mapped MITRE ATT&CK techniques include T1078.001 (Valid Accounts: Default Accounts), T1133 (External Remote Services), T1602 (Data from Configuration Repository), T1562.001 (Impair Defenses: Disable or Modify Tools), and T1588.006 (Obtain Capabilities: Vulnerabilities). CVSS 3.1 score (7.5, HIGH) is from NVD; vendor CVSS has not been published as of configuration date. EPSS score is 0.062% exploitation probability (19th percentile), indicating low current exploitation probability. The vulnerability is not currently listed in CISA KEV. CISA ICS advisory ICSA-26-160-03 has been published. Remediation is firmware upgrade to 002.006.000. Source authorities: CISA (T1), NVD (T1).

## Action Checklist

1. Step 1: Containment. Immediately isolate EcoStruxure Panel Server devices (PAS400, PAS600, PAS600V2, PAS800, PAS800V2) running firmware 002.005.000 or earlier from external network access. Disable cloud connectivity on affected units until firmware is upgraded, OR restrict cloud connectivity to trusted Schneider Electric management endpoints only, depending on operational requirements. Notify dependent cloud monitoring consumers of the restriction to prevent alerting cascades. Restrict management interface access to trusted internal hosts only using firewall rules or network segmentation. Reference CISA ICSA-26-160-03 for vendor-specific isolation guidance.
2. Step 2: Detection. Audit authentication logs on all EcoStruxure Panel Server units for successful logins using default credentials or logins occurring outside normal maintenance windows. Query SIEM for authentication events sourced from Panel Server IP ranges with anomalous success rates following failed attempts (NIST AU-6, CIS 8.2). Verify current firmware version on each device via management console; flag any unit reporting 002.005.000 or earlier as unpatched and at-risk. No public IOCs (IPs, hashes, domains) are associated with active exploitation at this time.
3. Step 3: Eradication. Upgrade all affected Panel Server firmware to version 002.006.000 per Schneider Electric's update procedure referenced in CISA ICSA-26-160-03. After upgrade, manually verify that device credentials are set to strong, unique values and are not factory defaults (NIST AC-2, CIS 4.7). Rotate any credentials that may have been exposed during a revert event. Apply credential hardening procedures (D3-CH, D3-CRO) immediately post-upgrade.
4. Step 4: Recovery. After firmware upgrade, confirm the device responds correctly to authentication with new credentials and rejects default credential attempts. Re-enable cloud connectivity only after credential state is validated. Monitor authentication logs for a minimum of 30 days post-remediation for anomalous login patterns (NIST AU-6, D3-LAM). Verify no unauthorized configuration changes were made during the exposure window by reviewing device configuration baselines (NIST CM, D3-SICA).
5. Step 5: Post-Incident. Conduct a review of all OT gateway devices across the environment for default credential exposure and insecure initialization practices. Establish automated firmware version monitoring and alerting for all ICS/OT devices (CIS 7.1, CIS 7.3). Implement network segmentation to ensure OT gateways are not directly reachable from untrusted networks without compensating controls (NIST AC-4, NIST AC-17). Subscribe to CISA ICS advisories for Schneider Electric products to reduce detection lag on future disclosures.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | URGENT |

| | |
|---|---|
| **Escalation Criteria** | Escalate to CISO, OT operations lead, and legal/compliance immediately if authentication logs on any Panel Server show a successful login from an unexpected source IP during the firmware exposure window (any period when firmware was 002.005.000 or earlier), or if post-upgrade configuration diff reveals unauthorized changes to ICS protocol mappings or cloud integration endpoints, as either condition indicates likely exploitation of CVE-2026-6866 and may trigger regulatory notification obligations under NERC CIP, TSA security directives, or sector-specific ICS incident reporting requirements. |
| **Recovery Notes** | After applying firmware 002.006.000 to all affected Panel Server models (PAS400, PAS600, PAS600V2, PAS800, PAS800V2), validate credential integrity by confirming factory-default login is rejected and new credentials authenticate successfully on each unit before restoring EcoStruxure cloud connectivity. Diff post-upgrade device configuration exports against pre-incident baselines to confirm no unauthorized changes to ICS data gateway mappings, connected field device registrations, or user accounts were introduced during the exposure window. Maintain elevated authentication log monitoring on all Panel Server units for a minimum of 30 days post-remediation, preserving logs for at least 90 days to support any retroactive forensic or regulatory review. |
| **Forensic Artifacts** | EcoStruxure Panel Server local authentication log (accessible via management console under System > Logs or equivalent): contains timestamped login events, source IPs, and success/failure status — the primary artifact for detecting unauthorized access via reverted default credentials during the CVE-2026-6866 exposure window. \| Panel Server firmware version string as reported in the management console UI and/or via the device REST API — documents the vulnerable state at time of discovery and confirms patch application; preserve as a screenshot or API response capture with timestamp. \| Full device configuration export (backup file) captured before and after firmware upgrade — diffs between these files reveal any ICS protocol mapping changes, cloud endpoint additions, or account modifications that an attacker with default-credential access could have made. \| Network traffic capture (pcpdump/PCAP) from the management interface of each Panel Server covering the exposure window — specifically looking for TCP sessions to EcoStruxure cloud endpoints (*.ecostruxure.se.com or per ICSA-26-160-03) initiated from or to the Panel Server, which would indicate active cloud-side exploitation or data exfiltration via the OT gateway. \| DHCP/ARP table records and firewall/ACL logs from the OT network boundary device covering the exposure window — identifies the source IPs of any hosts that successfully reached Panel Server management ports while factory defaults were active, supporting attribution and scope assessment. |

### Per-Action IR Details

**Step 1: Containment — Immediately isolate EcoStruxure Panel Server devices (PAS400, PAS600, PAS600V2, PAS800, PAS800V2) running firmware 002.005.000 or earlier from external network access. Disable cloud connectivity on affected units until firmware is upgraded. Restrict management interface access to trusted internal hosts only using firewall rules or network segmentation. Reference CISA ICSA-26-160-03 for vendor-specific isolation guidance.**

**NIST Phase:** Containment

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

**Controls:** NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

**Compensating:** On the upstream switch or router, apply an ACL or firewall rule blocking inbound/outbound TCP/UDP to the Panel Server management port (default HTTP/443 or vendor-specified port per ICSA-26-160-03) from all IPs except the designated jump host. Use `iptables -I FORWARD -d -j DROP` on a Linux gateway, or a

pfSense/OPNsense firewall rule, to block external reach. For cloud connectivity, physically disconnect or administratively disable the WAN-facing interface on the Panel Server via its local management console before network-layer controls are confirmed.

**Evidence:** Before isolating, capture a full netflow or tcpdump snapshot of traffic to/from each Panel Server IP: `tcpdump -i host -w panelserver_preiso_$(date +%Y%m%d%H%M).pcap`. Record any active sessions to the EcoStruxure cloud endpoint (*.ecostruxure.se.com or equivalent per ICSA-26-160-03) to identify whether an unauthorized actor was already connected using reverted default credentials at time of containment. Document the exact firmware version string visible in the management console before any changes are made.

**Step 2: Detection — Audit authentication logs on all EcoStruxure Panel Server units for successful logins using default credentials or logins occurring outside normal maintenance windows. Query SIEM for authentication events sourced from Panel Server IP ranges with anomalous success rates following failed attempts (NIST AU-6, CIS 8.2). Verify current firmware version on each device via management console; flag any unit reporting 002.005.000 or earlier as unpatched and at-risk. No public IOCs (IPs, hashes, domains) are associated with active exploitation at this time.**

**NIST Phase:** Detection Analysis

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

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

**Compensating:** Without a SIEM, export the Panel Server's local authentication log via its management interface (typically accessible under System > Logs > Authentication in EcoStruxure Panel Server UI per Schneider documentation). Parse the exported log file with: `grep -iE '(login|auth|success|default)' panelserver_auth.log | awk '{print $1,$2,$5,$7}' | sort | uniq -c | sort -rn` to surface repeated successful logins. Cross-reference login timestamps against your maintenance calendar. For firmware version auditing across multiple units, write a bash loop using `curl -sk https:///api/v1/firmware` (adjust endpoint per ICSA-26-160-03 API reference) to enumerate firmware strings without touching each console manually.

**Evidence:** Pull the Panel Server's local authentication/session log before any credential changes — this log will show successful authentications using the factory-default username/password pair (documented in Schneider's default credential disclosure within ICSA-26-160-03) and their source IP addresses. Capture DHCP lease records or static IP assignments for all Panel Server management interfaces to confirm the complete inventory of exposed devices. If the Panel Server exposes a syslog stream, preserve the raw syslog buffer on the receiving server covering the full period since the last confirmed firmware state.

**Step 3: Eradication — Upgrade all affected Panel Server firmware to version 002.006.000 per Schneider Electric's update procedure referenced in CISA ICSA-26-160-03. After upgrade, manually verify that device credentials are set to strong, unique values and are not factory defaults (NIST AC-2, CIS 4.7). Rotate any credentials that may have been exposed during a revert event. Apply credential hardening procedures (D3-CH, D3-CRO) immediately post-upgrade.**

**NIST Phase:** Eradication

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

**Controls:** NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

**Compensating:** Download firmware 002.006.000 from Schneider Electric's support portal (verify SHA checksum per ICSA-26-160-03 before flashing). Follow the Panel Server firmware update wizard in the local management console; do not attempt remote update over an untrusted path. Immediately post-upgrade, navigate to System > User Management in the Panel Server UI and set a unique password of at least 16 characters for every account — verify the default credential pair is rejected by attempting login with the factory defaults documented in the advisory. Record the credential change timestamp and operator identity in your incident log.

**Evidence:** Before applying the firmware upgrade, export a full device configuration backup from the Panel Server management console (System > Backup/Export or equivalent) — this preserves evidence of any configuration changes an unauthorized actor may have made while accessing the device via reverted default credentials. Hash the backup file with `sha256sum ` and store it as a forensic artifact. Document the firmware version string pre- and post-upgrade as confirmation of remediation.

**Step 4: Recovery — After firmware upgrade, confirm the device responds correctly to authentication with new credentials and rejects default credential attempts. Re-enable cloud connectivity only after credential state is validated. Monitor authentication logs for a minimum of 30 days post-remediation for anomalous login patterns (NIST AU-6, D3-LAM). Verify no unauthorized configuration changes were made during the exposure window by reviewing device configuration baselines (NIST CM, D3-SICA).**

**NIST Phase:** Recovery

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

**Controls:** NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), NIST AC-7 (Unsuccessful Logon Attempts), CIS 4.6 (Securely Manage Enterprise Assets and Software)

**Compensating:** Perform a structured credential validation test: attempt login to each Panel Server with the known factory-default credentials (per ICSA-26-160-03) and confirm rejection, then confirm successful login with the newly set credential — log both test results. Diff the post-upgrade configuration export against your pre-incident baseline using `diff baseline_config.json post_upgrade_config.json` to surface any unauthorized changes to ICS data mappings, cloud integration endpoints, or user accounts. Set a cron job or scheduled task to pull the Panel Server authentication log weekly for 30 days: `curl -sk -u : https:///api/v1/logs/auth >> /var/log/panelserver_monitor.log`.

**Evidence:** Capture a post-upgrade configuration export and diff it against the pre-incident baseline to identify any ICS protocol mappings, connected device registrations, or cloud endpoint configurations altered during the exposure window — a credential revert event on a gateway device like the Panel Server could have enabled an attacker to modify Modbus/IEC 61850/DNP3 data routing rules or add a rogue cloud integration. Preserve the 30-day post-remediation authentication log corpus as evidence of clean state for regulatory or insurance purposes.

**Step 5: Post-Incident — Conduct a review of all OT gateway devices across the environment for default credential exposure and insecure initialization practices. Establish automated firmware version monitoring and alerting for all ICS/OT devices (CIS 7.1, CIS 7.3). Implement network segmentation to ensure OT gateways are not directly reachable from untrusted networks without compensating controls (NIST AC-4, NIST AC-17). Subscribe to CISA ICS advisories for Schneider Electric products to reduce detection lag on future disclosures.**

**NIST Phase:** Post Incident

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

**Controls:** NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported)

**Compensating:** Build a lightweight OT asset firmware inventory using osquery's `SELECT * FROM system_info;` on any IT-OT boundary hosts, and supplement with a Nmap scan of OT VLAN management subnets (`nmap -sV -p 80,443, `) to enumerate EcoStruxure Panel Server devices and their reported firmware banners. For CISA advisory monitoring without a paid feed, configure an RSS reader or a free Python script using `feedparser` against CISA's ICS advisory RSS feed (https://www.cisa.gov/ics-advisories.xml — validate this URL before use) filtered on vendor keyword 'Schneider'. Document a quarterly firmware review cadence for all Schneider EcoStruxure Panel Server models in the OT asset register.

**Evidence:** The lessons-learned record for this incident should include: the full list of Panel Server devices by model and serial number, confirmed firmware versions at time of discovery, the duration of the exposure window (from last known good firmware state to patch application), and whether any authentication anomalies were detected in logs during that window. This record supports both internal risk management and any NERC CIP, IEC 62443, or sector-specific regulatory reporting obligations if the devices are in scope.

## Detection Guidance

No active exploitation IOCs (IP addresses, domains, file hashes) have been publicly disclosed as of the configuration date. Detection relies on behavioral and log-based indicators. Query authentication logs on EcoStruxure Panel Server management interfaces for: (1) successful authentications using known Schneider Electric factory default credentials; (2) successful logins immediately following a device reboot or power event, which may correlate with a credential revert trigger; (3) authentication source IPs outside your defined management subnets. Per NIST AU-6 and CIS 8.2, confirm audit logging is enabled and logs are forwarded to a centralized SIEM. Use D3-LAM (Local Account Monitoring) to baseline normal authentication patterns and alert on deviations. Cross-reference any Panel Server login events against T1078.001 (Default Accounts) detection rules in your SIEM. If network flow monitoring is in place, flag unexpected outbound connections from Panel Server IP ranges to external cloud endpoints, which may indicate unauthorized access following a credential revert event (T1133, T1602).

## Framework Mappings

### MITRE-ATTACK

- **T1078.001** — Default Accounts
- **T1588.006** — Vulnerabilities
- **T1562.001** — Disable or Modify Tools
- **T1602** — Data from Configuration Repository
- **T1133** — External Remote Services

### NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)

### OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

### HIPAA-SECURITY

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

### CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access

### SOC2-TSC

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

### 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 |
|---|---|---|
| T1078.001 | Default Accounts | Defense-Evasion |
| T1588.006 | Vulnerabilities | Resource-Development |
| T1562.001 | Disable or Modify Tools | Defense-Evasion |
| T1602 | Data from Configuration Repository | Collection |
| T1133 | External Remote Services | Persistence |

## Sources

| Source | URL | Tier |
|---|---|---|
| **ICS Advisories** | https://www.cisa.gov/news-events/ics-advisories/icsa-26-160-03 | T1 |
| | https://www.gerenciadeedificios.com/en/news/latest-news/375-enterpr... | T3 |
| **CVE-2026-6866 - CVE Record** | https://www.cve.org/CVERecord?id=CVE-2026-6866 | T3 |
| **CVE-2026-41266: Flowise Information Disclosure Flaw - SentinelOne** | https://www.sentinelone.com/vulnerability-database/cve-2026-41266/ | T3 |
| **CVE-2026-6866 - Red Hat Customer Portal** | https://access.redhat.com/security/cve/cve-2026-6866 | T3 |
| **NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-6866 | T1 |

Generated 2026-06-09 19:32 UTC by TJS Security Command Center