INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-09 19:31 UTC

Hard-Coded Credential and SQL Injection Flaws Affect 30+ Siemens KACO Blueplanet Solar Inverter Models, No Fix Planned

CVE VULNERABILITY | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0281
Type	CVE Vulnerability
CVE ID	CVE-2025-40946, CVE-2026-41125
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0002 (7th percentile)
Affected Products	Siemens KACO Blueplanet Inverters, 30+ models including blueplanet 100-165 TL3/NX3 series, blueplanet gridsafe series, blueplanet hybrid series (manufactured by KACO new energy GmbH / Siemens); deployed globally in energy sector critical infrastructure
Published	2026-06-09T12:00:00+00:00
Discovery Source	Rss:T2 Gov

Executive Summary

CISA advisory ICSA-26-160-02 discloses two vulnerabilities in Siemens KACO Blueplanet solar inverters affecting 30+ models deployed globally in energy sector critical infrastructure. The more severe flaw (CVE-2025-40946, CVSS 8.3) allows any network-accessible attacker to derive valid Technical Service credentials directly from a device serial number, bypassing authentication entirely. The vendor has confirmed no remediation is available for the majority of affected devices, leaving organizations dependent on compensating controls to protect operational technology assets with no patch remediation path.

Technical Analysis

CISA advisory ICSA-26-160-02 documents two vulnerabilities affecting 30+ Siemens KACO Blueplanet inverter models, including the blueplanet 100-165 TL3/NX3 series, gridsafe series, and hybrid series, manufactured by KACO new energy GmbH.

CVE-2025-40946 (CVSS 8.3, CWE-321/CWE-798): A hard-coded cryptographic key allows a network-adjacent or remote attacker to derive Technical Service credentials deterministically from a device serial number. No prior

authentication is required. Serial numbers are frequently discoverable via device labeling, public documentation, or network enumeration, making fleet-wide exploitation feasible. MITRE techniques: T1078.001 (Default Accounts), T1552.001 (Credentials In Files), T1046 (Network Service Discovery), T0885, T0866.

CVE-2026-41125 (CVSS 6.0, CWE-89): An SQL injection flaw enables local privilege escalation. Exploitable by a locally authenticated attacker. MITRE techniques: T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1059.

Patch status: The vendor has indicated no fix exists or is planned for the majority of affected devices. Compensating controls are the only available mitigation. Source: CISA ICS Advisory ICSA-26-160-02.

Action Checklist

1. Step 1: Containment, Immediately isolate all Siemens KACO Blueplanet inverter models (including blueplanet 100-165 TL3/NX3, gridsafe, and hybrid series) from direct internet and untrusted network access. Place affected devices behind a dedicated OT network segment with default-deny firewall rules. Disable any remote management interfaces exposed outside the OT DMZ. Reference: CISA ICSA-26-160-02 mitigation section. Maps to NIST AC-4 (Information Flow Enforcement) and CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Audit network logs for unexpected authentication attempts or successful logins to inverter management interfaces, particularly from IP addresses outside authorized OT management segments. Query SCADA/historian and inverter management system logs for Technical Service account activity. Search for serial number enumeration patterns in network traffic (T1046). If a SIEM is ingesting OT logs, create alerts on Technical Service account logins correlated with previously unseen source IPs. Maps to NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, No vendor patch is available for the majority of affected devices. Apply the following compensating controls per CISA ICSA-26-160-02: (a) restrict network access to inverter management interfaces to named authorized hosts only; (b) rotate or invalidate any Technical Service credentials where the vendor interface permits; (c) disable unused network services on affected devices where configurable. Maps to NIST AC-17 (Remote Access), AC-6 (Least Privilege), and D3-CRO (Credential Rotation), D3-CH (Credential Hardening).
4. Step 4: Recovery, After compensating controls are applied, validate that inverter management interfaces are no longer reachable from untrusted network segments using a port scan from outside the OT segment. Confirm Technical Service account activity returns to baseline in logs. Enable continuous monitoring on affected device interfaces and set alerts for any re-exposure. Review firewall rule changes with OT engineering before restoring full operational status. Maps to NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 7.1 (Establish and Maintain a Vulnerability Management Process).
5. Step 5: Post-Incident, Document the control gap: OT assets with no vendor remediation path require a formal exception process and compensating control register entry. Assess whether serial numbers for affected inverters are publicly discoverable (documentation, asset management systems, vendor portals) and restrict access. Evaluate OT asset inventory for other devices sharing similar hard-coded credential patterns. Update the vulnerability management process to flag no-fix advisories for critical infrastructure assets separately. Maps to NIST AC-2 (Account Management), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), and D3-UAP (User Account Permissions).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to OT security leadership and legal/compliance if Technical Service account authentication events are confirmed from unauthorized source IPs, if SCADA historian data shows inverter parameter changes during the exposure window, or if affected inverters are classified under NERC CIP or other critical infrastructure regulatory frameworks requiring mandatory incident notification — the combination of CVSS 8.3, no vendor fix, and direct authentication bypass in energy sector critical infrastructure meets the threshold for senior leadership and regulatory notification without delay.
Recovery Notes	Post-containment, continuously validate network segmentation controls for a minimum of 30 days using automated daily port scans from outside the OT segment, as firewall misconfigurations or OT change management gaps could re-expose inverter management interfaces without detection. Monitor SCADA historian operational parameter trends for all affected inverters over the same 30-day period to detect any latent configuration manipulation that may have been introduced before containment — anomalies in power output curves, frequency response, or reactive power setpoints are the primary operational indicators of pre-containment inverter tampering. Because no vendor patch is planned for the majority of affected models, recovery is a permanent compensating control posture, not a point-in-time fix; schedule quarterly reviews of network segmentation rules and serial number access controls as standing operational requirements.
Forensic Artifacts	Inverter management interface authentication logs — specifically all Technical Service account login events with source IP, timestamp, and session outcome; under CVE-2025-40946 the attacker derives valid credentials from the serial number, so any Technical Service login from a non-authorized IP is a high-confidence exploitation indicator | PCAP from the OT network segment covering the exposure window — search for HTTP/HTTPS requests to inverter management URIs containing serial number strings in parameters or headers, which represents the reconnaissance phase of CVE-2025-40946 credential derivation | SCADA historian configuration change records for all affected KACO Blueplanet inverters — an attacker authenticating as Technical Service would have write access to operational parameters; historian diffs showing changes to power limits, grid feed-in thresholds, or protection relay setpoints are direct evidence of post-authentication manipulation | Inverter management interface web server access logs (if accessible via device CLI or management interface export) — for CVE-2026-41125 SQL injection, look for URI-encoded SQL metacharacters (%27, %3B, UNION, SELECT) in GET/POST request parameters to the inverter's reporting or query endpoints | OT network firewall and router connection logs for the period from CISA ICSA-26-160-02 publication date through containment — enumerate all unique source IPs that established TCP sessions to inverter management ports (80, 443, or device-specific management ports) to identify the full scope of external access during the vulnerability exposure window

Per-Action IR Details

Step 1: Containment — Immediately isolate all Siemens KACO Blueplanet inverter models (including blueplanet 100–165 TL3/NX3, gridsafe, and hybrid series) from direct internet and untrusted network access. Place affected devices behind a dedicated OT network segment with default-deny firewall rules. Disable any remote management interfaces exposed outside the OT DMZ. Reference: CISA ICSA-26-160-02 mitigation section. Maps to NIST AC-4 (Information Flow Enforcement) and 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), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Use iptables or Windows Firewall (on any intermediate jump host or OT gateway) to implement a default-deny ACL permitting only named authorized management workstation IPs to reach the inverter web management port (typically TCP 443 or TCP 80). Command example: `iptables -I FORWARD -d -j DROP` followed by `iptables -I FORWARD -s -d -j ACCEPT`. Run `nmap -sS -p 80,443,22,502,2404 ` from outside the OT segment before and after the rule change to confirm the management interface is no longer reachable. Two-person verification: one engineer applies rules, the second independently validates reachability.

Evidence: Before isolating, capture a full packet capture (Wireshark/tcpdump) of current traffic to/from each affected inverter's management interface IP to preserve a baseline and any pre-existing attacker sessions. Record the inverter's current active TCP sessions: `ss -tnp` or equivalent on the OT gateway. Export the inverter management system (IMS) or SCADA historian connection logs for the 30 days prior to isolation, specifically preserving all source IPs that successfully authenticated to Technical Service accounts — these are the primary indicator of CVE-2025-40946 exploitation.

Step 2: Detection — Audit network logs for unexpected authentication attempts or successful logins to inverter management interfaces, particularly from IP addresses outside authorized OT management segments. Query SCADA/historian and inverter management system logs for Technical Service account activity. Search for serial number enumeration patterns in network traffic (T1046). If a SIEM is ingesting OT logs, create alerts on Technical Service account logins correlated with previously unseen source IPs. Maps to NIST AU-6 (Audit Record Review, Analysis, and Reporting) and 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-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use grep or PowerShell to parse inverter management system authentication logs for 'Technical Service' account login events: `grep -i 'technical service\|techservice' /var/log/inverter-mgmt/*.log | grep -v "`. For serial number enumeration consistent with MITRE T1046 (Network Service Discovery), run Wireshark with display filter `tcp.port == 80 || tcp.port == 443` against a span/mirror port on the OT switch and search for GET/POST requests containing serial number patterns (typically alphanumeric strings matching KACO device naming conventions). Write a Sigma rule targeting authentication log fields: condition on account name matching Technical Service AND source IP NOT in authorized_hosts list, exportable to any log tool.

Evidence: Collect the full authentication logs from the Siemens KACO Blueplanet inverter management interface or connected IMS for all Technical Service account login events, noting source IP, timestamp, and session duration. Retrieve any SCADA historian records of configuration change events or parameter write operations initiated via Technical Service credentials, which would indicate an attacker moved from authentication to manipulation. Preserve raw PCAP showing HTTP/HTTPS requests to the inverter management URI containing serial number values in request parameters or headers, as this is the specific network artifact produced by CVE-2025-40946 credential derivation reconnaissance (attacker must first obtain or enumerate serial numbers before deriving credentials).

Step 3: Eradication — No vendor patch is available for the majority of affected devices. Apply the following compensating controls per CISA ICSA-26-160-02: (a) restrict network access to inverter management interfaces to named authorized hosts only; (b) rotate or invalidate any Technical Service credentials where the vendor interface permits; (c) disable unused network services on affected devices where configurable. Maps to NIST AC-17 (Remote Access), AC-6 (Least Privilege), and D3-CRO (Credential Rotation), D3-CH (Credential Hardening).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), NIST AC-7 (Unsuccessful Logon Attempts)

Compensating: Because CVE-2025-40946 derives Technical Service credentials deterministically from the device serial number and no firmware patch exists, credential rotation alone is insufficient if the derivation algorithm is unchanged — document this residual risk explicitly. Where the inverter management interface permits, disable the Technical Service account entirely if operational monitoring functions can be maintained through a separate read-only or operator-tier account. Run `nmap -sV -p 1-65535 ` to enumerate all listening services and document each; disable any non-essential services (FTP, Telnet, unnecessary HTTP endpoints) directly on the device if the firmware configuration interface allows. For SQL injection exposure under CVE-2026-41125, restrict any web-accessible query or reporting interface to localhost or the named authorized management host, eliminating the network-reachable attack surface in the absence of a patch.

Evidence: Before credential rotation or service disablement, capture the current device configuration via the management interface (export running config if supported) and hash the file (SHA-256) to establish a pre-change baseline. Document which network services were active on each inverter model (nmap output), as post-eradication comparison will confirm attack surface reduction. If the inverter management interface logs configuration change events, export and preserve those logs immediately — any attacker who exploited CVE-2025-40946 prior to your response may have altered inverter operating parameters (power limits, grid feed-in thresholds), and a configuration diff between the baseline export and current state reveals unauthorized changes.

Step 4: Recovery — After compensating controls are applied, validate that inverter management interfaces are no longer reachable from untrusted network segments using a port scan from outside the OT segment. Confirm Technical Service account activity returns to baseline in logs. Enable continuous monitoring on affected device interfaces and set alerts for any re-exposure. Review firewall rule changes with OT engineering before restoring full operational status. Maps to NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

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), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Conduct external validation with `nmap -sS -p 80,443,22,502,2404 ` executed from a host outside the OT segment (e.g., corporate LAN or a dedicated test VLAN) — all management ports must show 'filtered' or 'closed', not 'open'. For continuous monitoring without a SIEM, configure a cron job on the OT gateway to run this nmap scan daily and diff the output against the post-remediation baseline: `nmap -oN /tmp/scan_$(date +%F).txt && diff /tmp/scan_baseline.txt /tmp/scan_$(date +%F).txt >> /var/log/ot_exposure_monitor.log`. Alert on any diff output via email or syslog. Validate inverter operational parameters (output power, grid sync values) through the SCADA historian to confirm no configuration tampering occurred during the exposure window.

Evidence: Retain pre- and post-remediation nmap scan outputs as timestamped evidence of attack surface reduction for audit and regulatory purposes. Preserve inverter management authentication logs covering the entire exposure window (from initial CVE disclosure or earliest possible exploitation date through containment) with AU-11-compliant retention — do not allow log rotation to delete these records. Collect SCADA historian trend data for each affected inverter's operational parameters (MW output, frequency response, reactive power) over the exposure window to support forensic determination of whether any attacker-driven parameter changes affected grid operations.

Step 5: Post-Incident — Document the control gap: OT assets with no vendor remediation path require a formal exception process and compensating control register entry. Assess whether serial numbers for affected inverters are publicly discoverable (documentation, asset management systems, vendor portals) and restrict access. Evaluate OT asset inventory for other devices sharing similar hard-coded credential patterns. Update the vulnerability management process to flag no-fix advisories for critical infrastructure assets separately. Maps to NIST AC-2 (Account Management), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), and D3-UAP (User Account Permissions).

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), NIST AC-1 (Policy And Procedures), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a serial number exposure audit: search internal documentation repositories (SharePoint, Confluence, asset management DB), vendor portal accounts, and any public-facing maintenance records for KACO Blueplanet serial numbers — serial numbers are the direct input for deriving Technical Service credentials under CVE-2025-40946, so their confidentiality is now a security control. Use osquery to query the enterprise asset inventory database: `SELECT * FROM assets WHERE model LIKE '%blueplanet%' OR manufacturer LIKE '%KACO%';` and cross-reference against CISA ICSA-26-160-02's affected model list. Create a 'no-fix advisory' tracking category in your vulnerability management process (spreadsheet acceptable for small teams) with mandatory fields: compensating control owner, review frequency, and regulatory reporting obligation — this directly addresses the permanent residual risk posture for these 30+ device models.

Evidence: Compile a formal record of all Technical Service account authentication events observed during the exposure window, including source IPs, timestamps, and any correlated configuration changes, to support potential NERC CIP or sector-specific regulatory reporting obligations if the affected inverters are part of a bulk electric system. Document the serial number inventory and all locations where serial numbers were found to be accessible (internal or external), as this constitutes evidence of the pre-existing control gap that enabled CVE-2025-40946's attack vector. Preserve the compensating control register entries, network segmentation rule changes, and post-remediation scan outputs as the formal audit trail demonstrating due diligence in the absence of a vendor-provided fix.

Detection Guidance

Primary detection focus is unauthorized Technical Service account authentication on affected inverter management interfaces.

1. Log sources: Inverter management system logs, SCADA historian, OT network firewall/IDS logs, and any centralized syslog forwarding from the OT segment.

2. Behavioral indicators:

- Technical Service account login events from IP addresses outside the authorized OT management host list (T1078.001, T1046)

- Authentication attempts correlated with serial number patterns in payloads or request parameters (T1046, T0885)

- Unusual POST or query activity against inverter management web interfaces (T1190, CWE-89 SQL injection pattern)

- Privilege changes or configuration modifications following a Technical Service login

- Sequential connection attempts across multiple inverter IP addresses in the OT subnet (fleet enumeration pattern)

3. SIEM query guidance: Alert on Technical Service account logins where source IP is not in the authorized management host allowlist. Alert on any authentication success outside business hours on inverter management interfaces.

4. Network-level: Inspect traffic to inverter management ports for SQL metacharacter sequences in request bodies (single quotes, UNION statements, comment sequences) as indicators of CVE-2026-41125 exploitation attempts.

5. Limitation: No public exploit code or IOCs have been released as of the ICSA-26-160-02 advisory release date (approximately June 9, 2026). Detection relies on behavioral baselines and log analysis, not signature matching. Organizations should monitor vendor and CISA security feeds for emergence of exploit tooling. Maps to NIST AU-2 (Event Logging), AU-6 (Audit Record Review), and D3-LAM (Local Account Monitoring).

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1078.001** — Default Accounts
- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter
- **T0885** — Commonly Used Port
- **T1068** — Exploitation for Privilege Escalation
- **T1110.001** — Password Guessing
- **T0866** — Exploitation of Remote Services
- **T1552.001** — Credentials In Files
- **T1046** — Network Service 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-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-10** — Information Input Validation
- **AT-2** — Literacy Training and Awareness
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography
- **A.5.23** — Information security for use of cloud services

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
- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1078.001	Default Accounts	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T0885	Commonly Used Port	Command-And-Control
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1110.001	Password Guessing	Credential-Access
T0866	Exploitation of Remote Services	Initial-Access
T1552.001	Credentials In Files	Credential-Access
T1046	Network Service Discovery	Discovery

Sources

Source	URL	Tier
ICS Advisories	https://www.cisa.gov/news-events/ics-advisories/icsa-26-160-02	T1
	https://taiyangnews.info/technology/kaco-new-energy-string-inverter...	T3
	https://www.pv-magazine.com/2023/08/17/siemens-to-open-u-s-utility-...	T3
	https://taiyangnews.info/technology/kaco-siemens-string-inverter-in...	T3
CVE-2025-40946: Siemens Blueplanet Auth Bypass Flaw	https://www.sentinelone.com/vulnerability-database/cve-2025-40946/	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-40946, CVE-2026-41125	T1

Generated 2026-06-09 19:31 UTC by TJS Security Command Center