INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-30 14:01 UTC

CISA Releases 11 ICS Advisories Covering Maritime, Building Automation, CCTV, EV Charging, and Industrial OT Systems (May 28, 2026)

GOVERNANCE | HIGH

SCC Item ID	SCC-GOV-2026-0042
Type	Governance
Severity	HIGH
Affected Products	MacGregor Voyage Data Recorder (VDR) G4e, ABB EIBPORT, ABB Busch-Welcome 2 Wire Door Opener Actuator, CP Plus 8 Ch. Network Video Recorder, KMW CCTV Security Cameras, Schneider Electric EcoStruxure Machine Expert HVAC, XCharge C6 EV Charger, Fourth Frontier Frontier X Mobile Application, Fourth Frontier Frontier X2, Mitsubishi Electric Factory Automation Engineering Products, ABB Ability Zenon Remote Transport
Published	2026-05-28
Discovery Source	Gemini

Executive Summary

On May 28, 2026, CISA published 11 ICS advisories covering vulnerabilities across 11 products from 7 vendors, spanning maritime, building automation, physical security, EV charging, industrial manufacturing, and cardiac monitoring sectors. Affected systems operate in critical infrastructure environments where unpatched vulnerabilities can disrupt operations, compromise physical security controls, or expose sensitive operational data. Organizations running any of the named products should review the individual CISA advisories immediately and apply vendor mitigations, as these systems are often network-accessible and difficult to patch quickly in operational environments.

Technical Analysis

CISA released 9 new ICS advisories and 2 updates on May 28, 2026, covering the following products: MacGregor Voyage Data Recorder (VDR) G4e (maritime black box), ABB EIBPORT (smart building automation hub, with session hijack risk reported), ABB Busch-Welcome 2 Wire Door Opener Actuator (physical access control), CP Plus 8-Channel Network Video Recorder (surveillance), KMW CCTV Security Cameras (surveillance), Schneider Electric EcoStruxure Machine Expert HVAC (industrial HVAC automation), XCharge C6 EV Charger (EV charging infrastructure), Fourth Frontier Frontier X and X2 (cardiac monitoring wearables),

Mitsubishi Electric Factory Automation Engineering Products (manufacturing OT), and ABB Ability Zenon Remote Transport (transport infrastructure automation). Specific CVE identifiers were not extractable from available secondary sources; canonical CVE data resides in each discrete CISA advisory at cisa.gov/news-events/ics-advisories. The ABB EIBPORT advisory references session hijack risk, suggesting insufficient session management controls. MITRE ATT&CK techniques associated with this advisory bundle include T1190 (Exploit Public-Facing Application), T1498 (Network Denial of Service), and T1200 (Hardware Additions). No CVSS scores or EPSS data are available from current sources. No CISA KEV entries are associated with this bundle at time of publication. Confidence in vendor and product scope is medium, derived from secondary reporting; all technical details should be verified against the primary CISA advisories.

Action Checklist

1. Step 1: Containment, Identify all instances of the 11 affected products in your environment using your asset inventory (CIS 1.1). Prioritize internet-facing or network-accessible deployments. For ABB EIBPORT systems with confirmed session hijack risk, restrict network access at the perimeter immediately pending patch review. Segment OT/ICS assets from corporate IT networks where not already done (NIST AC-4).
2. Step 2: Detection, Review logs on all affected OT and IoT devices for anomalous session activity, unexpected configuration changes, or unauthorized access attempts (NIST AU-6, AU-2). For ABB EIBPORT, look for session token reuse or concurrent sessions from different source IPs (NIST AC-10). Check network traffic logs for unexpected outbound connections from the affected device IP ranges. Query your SIEM for access events involving the specific asset hostnames or IP addresses of the 11 product types.
3. Step 3: Eradication, Retrieve and apply vendor-specific mitigations from each of the 11 individual CISA advisories at cisa.gov/news-events/ics-advisories. Specific patch IDs and firmware update paths are documented in each advisory. Apply patches according to vendor guidance; where patching is not immediately feasible in OT environments, implement compensating controls such as network segmentation, access restrictions, and monitoring (NIST SI-4, CIS 7.3, CIS 7.4).
4. Step 4: Recovery, After applying mitigations, verify system integrity by reviewing current session states, active user accounts, and configuration baselines on affected devices (NIST AC-2, D3-SFA). Restore normal operations only after confirming no unauthorized changes were made. Enable or verify enhanced logging on remediated systems and monitor for recurrence of anomalous activity for at least 30 days post-patching (NIST AU-12, CIS 8.2).
5. Step 5: Post-Incident, Conduct a gap assessment against your OT/ICS asset inventory to verify completeness of coverage for these product families (CIS 1.1). Review network segmentation controls separating OT from IT environments (NIST AC-4, AC-17). Evaluate whether MFA is enforced on administrative access to affected systems (CIS 6.5, D3-MFA). Document this advisory bundle in your vulnerability management process and update your remediation timelines (CIS 7.1, CIS 7.2).

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to CISO and legal counsel if any ABB EIBPORT session hijack indicators are confirmed in logs, if Fourth Frontier Frontier X or X2 cardiac monitoring PHI exposure cannot be ruled out (HIPAA breach notification clock starts at discovery), or if MacGregor VDR G4e on a vessel under SOLAS compliance obligations shows any evidence of data tampering, as these conditions trigger regulatory notification requirements beyond standard IR SLAs.
Recovery Notes	After patching, validate OT system integrity by diffing running device configurations against pre-incident baselines — specifically, compare ABB EIBPORT KNX automation logic, Schneider EcoStruxure HVAC control setpoints, and Mitsubishi FA PLC ladder logic against last known-good backups to detect any unauthorized modifications made during the exposure window. Monitor network traffic from all 11 product IP ranges for 30 days post-patch using hourly packet captures or NetFlow records, specifically watching for unexpected outbound connections, RTSP stream pulls to external IPs from CP Plus NVR and KMW cameras, and any reconnection attempts to the ABB EIBPORT on previously-blocked ports. If the MacGregor VDR G4e was network-accessible during the exposure window on a vessel subject to flag state or port state control inspections, notify the vessel operator's designated person ashore (DPA) and document the exposure period for inclusion in any upcoming ISM Code audit.
Forensic Artifacts	ABB EIBPORT session logs: authentication records showing session token values, source IPs, and timestamps — the forensic indicator for the session hijack vulnerability is the same session cookie or token value appearing from two or more distinct source IP addresses within a single session lifetime, exportable from the device's embedded web server log (typically /var/log/ on Linux-based EIBPORT hardware). | CP Plus 8-Ch NVR and KMW CCTV camera RTSP access logs: records of RTSP stream session initiations (DESCRIBE, SETUP, PLAY method requests) logged by the NVR's access control module — unauthorized stream pulls to non-inventory external IPs are the primary forensic indicator of exploitation of camera or NVR vulnerabilities in this advisory set. | Mitsubishi Electric FA engineering workstation Windows Event Logs: Security Event Log entries for Event ID 4648 (Logon using explicit credentials) and Event ID 4698 (Scheduled task created) on workstations running MELSOFT, GX Works, or other affected Mitsubishi FA engineering software, combined with file system last-modified timestamps on .gx3/.gxw project files stored in the engineering workstation's project directory. | Fourth Frontier Frontier X and X2 mobile application data egress records: MDM platform logs (Intune, Jamf, or equivalent) or mobile network firewall logs showing data transmission events from the Frontier X app to remote endpoints during the exposure window — relevant for PHI breach assessment if the app was used in an occupational health or clinical monitoring context and transmitted biometric or cardiac data to unauthorized destinations. | OT network NetFlow or packet captures from the VLAN or network segment hosting Schneider EcoStruxure Machine Expert HVAC and XCharge C6 EV charger management interfaces: baseline-comparison captures showing any new destination IPs, unexpected protocol usage, or abnormal session volumes on the management ports (typically TCP 443, 8080, or vendor-specific engineering ports) that appeared during the advisory exposure window.

Per-Action IR Details

Step 1: Containment — Identify all instances of the 11 affected products in your environment using your asset inventory (CIS 1.1). Prioritize internet-facing or network-accessible deployments. For ABB EIBPORT systems with confirmed session hijack risk, restrict network access at the perimeter immediately pending patch review. Segment OT/ICS assets from corporate IT networks where not already done (NIST AC-4).

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST IR-4 (Incident Handling), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run a Nmap scan against your RFC 1918 ranges targeting ports commonly used by each affected product (ABB EIBPORT typically TCP 443/80, CP Plus NVR TCP 80/554/8000, XCharge C6 TCP 443/8080, Mitsubishi MELSOFT TCP 5007/5008). Use 'nmap -sV -p 80,443,554,5007,5008,8000,8080 192.168.0.0/16 --open -oN ics_discovery.txt' and cross-reference output against known device hostnames or MAC OUI prefixes (ABB OUIs: 00:0A:DC, 00:04:AC; Schneider OUIs: 00:80:F4). For ABB EIBPORT specifically, block TCP 443 inbound at your perimeter firewall using an ACL rule while patch review is underway.

Evidence: Before isolating any ABB EIBPORT device, capture current active session table from the device's web interface or management API (GET /api/sessions or equivalent) and export to a timestamped file. Document all source IPs currently holding authenticated sessions. For OT network segments, capture a 15-minute Wireshark packet capture on the SPAN or mirror port serving the OT VLAN to preserve a pre-containment baseline of normal Modbus, BACnet, or proprietary protocol traffic from Schneider EcoStruxure and Mitsubishi FA devices before segmentation cuts visibility.

Step 2: Detection — Review logs on all affected OT and IoT devices for anomalous session activity, unexpected configuration changes, or unauthorized access attempts (NIST AU-6, AU-2). For ABB EIBPORT, look for session token reuse or concurrent sessions from different source IPs (NIST AC-10). Check network traffic logs for unexpected outbound connections from the affected device IP ranges. Query your SIEM for access events involving the specific asset hostnames or IP addresses of the 11 product types.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AC-10 (Concurrent Session Control), NIST SI-4 (System Monitoring)

Compensating: For teams without SIEM: On the ABB EIBPORT management interface, manually export the authentication and session logs (typically found at /var/log/eibport/ or equivalent embedded Linux path) and grep for concurrent session entries: 'grep -E "session|login|auth" /var/log/eibport/*.log | awk '{print $1,$2,$NF}' | sort | uniq -d'. For CP Plus NVR, pull the device event log via the NVR's local web UI under System > Logs > Access Log and filter for login events outside business hours. For network-level detection without SIEM, run Zeek (formerly Bro) in offline mode against the pre-containment packet capture to extract conn.log and http.log, then filter for HTTP sessions to the EIBPORT IP with mismatched User-Agent strings or session cookies appearing from multiple source IPs within the same 5-minute window.

Evidence: Preserve the following before any log rotation occurs: (1) ABB EIBPORT web server access logs showing session token values, source IPs, and timestamps — look specifically for the same session token (cookie value) appearing from two or more different source IP addresses, which is the forensic signature of a session hijack against this product. (2) For CP Plus 8-Ch NVR and KMW CCTV cameras, pull RTSP stream access logs and look for unauthorized stream pulls to external IPs — a successful exploit against these products would manifest as unexpected RTSP session initiations to non-inventory IPs. (3) For Mitsubishi Electric FA Engineering Products (MELSOFT, GX Works), check Windows Security Event Log on engineering workstations for Event ID 4648 (Logon using explicit credentials) and Event ID 4624 (Type 3 network logon) from unexpected accounts accessing the Mitsubishi project file directories.

Step 3: Eradication — Retrieve and apply vendor-specific mitigations from each of the 11 individual CISA advisories at cisa.gov/news-events/ics-advisories. Specific patch IDs and firmware update paths are documented in each advisory. Apply patches according to vendor guidance; where patching is not immediately feasible in OT environments, implement compensating controls such as network segmentation, access restrictions, and monitoring (NIST SI-4, CIS 7.3, CIS 7.4).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-4 (System Monitoring), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch

Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For OT environments where live patching is not feasible (MacGregor VDR G4e on active vessels, Schneider EcoStruxure in live production, Mitsubishi FA systems on running lines): implement a VLAN-based micro-segmentation compensating control using existing managed switch ACLs to permit only whitelisted management IPs to communicate with each affected device. Document the compensating control with an exception ticket referencing the specific CISA advisory ID. For XCharge C6 EV chargers that cannot be taken offline, disable the remote management interface at the charger's local HMI if that option exists, and block all inbound connections to the charger management port (typically TCP 443 or 8080) at the nearest upstream firewall. Set a calendar reminder for the next maintenance window with the specific firmware version required per each CISA advisory.

Evidence: Before applying any firmware update or patch: (1) For MacGregor VDR G4e, export a full backup of the VDR configuration and recorded data package — the VDR stores voyage data that may be legally required under SOLAS and could constitute forensic evidence of any data manipulation if the device was compromised. (2) For ABB EIBPORT, export the current EIB/KNX group address configuration and any automation scripts before patching — a threat actor with session hijack access may have modified building automation logic (e.g., altered access control schedules, HVAC setpoints) and this pre-patch baseline is your only comparison point. (3) For Schneider EcoStruxure Machine Expert HVAC, back up the current project file (.m6p or .ecp format) from the programming workstation before applying the patch to detect any unauthorized logic modifications.

Step 4: Recovery — After applying mitigations, verify system integrity by reviewing current session states, active user accounts, and configuration baselines on affected devices (NIST AC-2, D3-SFA). Restore normal operations only after confirming no unauthorized changes were made. Enable or verify enhanced logging on remediated systems and monitor for recurrence of anomalous activity for at least 30 days post-patching (NIST AU-12, CIS 8.2).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AU-12 (Audit Record Generation), NIST AU-11 (Audit Record Retention), NIST CP-10 (System Recovery and Reconstitution), CIS 8.2 (Collect Audit Logs), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: For post-patch integrity verification without enterprise tooling: (1) On ABB EIBPORT, immediately after patching, pull the full user account list from the device management interface and compare against your known-good baseline — look for any accounts created during the window of exposure. (2) For CP Plus NVR and KMW CCTV cameras, review the camera access control list (ACL) for any new IP addresses added as trusted viewers or administrators. (3) For Mitsubishi Electric FA products, re-open the engineering project in GX Works or MELSOFT and use the built-in 'Compare with PLC' function to diff the running PLC program against your last known-good backup — any ladder logic or structured text differences are a high-priority finding. (4) Set up a lightweight Zeek or tcpdump cron job ('tcpdump -i eth0 -w /logs/ot_monitor_$(date +%Y%m%d_%H).pcap -G 3600 host [device_IP]') on a jump host or Linux VM to capture hourly PCAPs from each remediated device for the 30-day monitoring window.

Evidence: Post-remediation evidence to retain for the 30-day monitoring window: (1) For ABB EIBPORT, retain session logs showing the post-patch session token format change (if the patch invalidates existing tokens, the log will show a forced re-authentication event for all users — absence of this event for a specific user may indicate a persistent backdoor session). (2) For Fourth Frontier Frontier X and X2 cardiac monitoring mobile applications, if deployed in a healthcare or occupational health context, verify that any health data transmitted from the app during the exposure window is accounted for — check mobile device management (MDM) logs for data egress events from the Frontier X app to non-authorized endpoints, and flag for potential HIPAA breach assessment if PHI was in scope.

Step 5: Post-Incident — Conduct a gap assessment against your OT/ICS asset inventory to verify completeness of coverage for these product families (CIS 1.1). Review network segmentation controls separating OT from IT environments (NIST AC-4, AC-17). Evaluate whether MFA is enforced on administrative access to affected systems (CIS 6.5, D3-MFA). Document this advisory bundle in your vulnerability management process and update your remediation timelines (CIS 7.1, CIS 7.2).

NIST Phase: Post Incident

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), NIST RA-3 (Risk Assessment), NIST SI-2 (Flaw Remediation), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For the OT/ICS asset inventory gap assessment: export your current CMDB or asset spreadsheet and run a vendor-name search for 'MacGregor', 'ABB', 'CP Plus', 'KMW', 'Schneider Electric', 'XCharge', 'Fourth Frontier', and 'Mitsubishi Electric' — any assets matching these vendors that are NOT already in your patching queue represent inventory gaps. For MFA gap assessment on systems that do not natively support MFA (many OT devices in this advisory set do not): document these as compensating control candidates and implement network-layer MFA enforcement via a VPN gateway or jump host with MFA (e.g., WireGuard + Duo free tier) that gates all administrative access to the OT segment, rather than relying on device-native MFA. Commit findings to a lessons-learned document using the NIST 800-61r3 §4 lessons-learned template structure.

Evidence: Post-incident documentation artifacts to retain: (1) The pre- and post-segmentation network diagrams showing the OT/IT boundary state before and after this advisory response — these serve as evidence of control improvement for any subsequent audit or regulatory review. (2) For the Fourth Frontier Frontier X and X2 cardiac monitoring devices, retain a written determination of whether any PHI was processed on the affected application version during the exposure window, as this determination drives HIPAA breach notification obligations independent of whether active exploitation is confirmed. (3) The completed asset inventory query results showing all instances found (or not found) of each of the 11 product families — a negative finding ('zero instances of KMW CCTV found') is as valuable as a positive one and should be retained as evidence of scope assessment.

Detection Guidance

No specific CVE identifiers or confirmed IOCs are available from current sources; detection guidance is based on the product types and the one confirmed vulnerability characteristic (ABB EIBPORT session hijack). Query your SIEM and asset management tools for any of the 11 affected product names in your inventory. For ABB EIBPORT: look for concurrent active sessions from distinct source IPs, session tokens appearing in multiple request streams, or administrative access outside normal change windows (relevant to NIST AC-10, AU-6). For NVR and CCTV products (CP Plus, KMW): check for configuration changes, unexpected firmware update events, or anomalous outbound connections. For maritime VDR (MacGregor G4e): if network-accessible, review access logs for unauthorized read or write events to recorded data. For EV charging infrastructure (XCharge C6): monitor for unexpected API calls or firmware modification events. For OT/industrial products (Schneider EcoStruxure, Mitsubishi Factory Automation, ABB Zenon): alert on any engineering workstation connections outside maintenance windows (T1190 relevant). Review ICS network monitoring tools (if deployed) for lateral movement patterns consistent with T1190 or T1200. Verify against individual CISA advisories for product-specific detection indicators once CVE details are available.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1498** — Network Denial of Service
- **T1200** — Hardware Additions

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
- **SI-4** — System Monitoring

ISO-27001-2022

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

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1498	Network Denial of Service	Impact
T1200	Hardware Additions	Initial-Access

Sources

Source	URL	Tier
9 Advisories and 2 Updates Published – 5-28-26	https://patrickcoyle.substack.com/p/9-advisories-and-2-updates-publ...	T3
VDR G4[e] S-VDR G4[e]	https://www.macgregor.com/globalassets/picturepark/imported-assets/...	T3
MacGregor Voyage Data Recorder VDR G4e and S- ...	https://static.mackaycomm.com/wp-content/uploads/2021/08/Mackay-Mar.. .	T3
ICS Advisories	https://www.cisa.gov/news-events/ics-advisories	T1
ABB Smart Building Hubs Expose Session Hijack Risk	https://www.si-news.ai/article/abb-eibport-4aef3060c383beb5	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-30 14:01 UTC by TJS Security Command Center