INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-05 19:18 UTC

900+ US ATG Systems Actively Compromised: Fuel Infrastructure Under Sustained Attack

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0416
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Automatic Tank Gauge (ATG) systems (multiple vendors including Franklin Fueling, Veeder-Root, OPW); internet-exposed ICS/SCADA fuel management systems at US gas stations and critical infrastructure sites
Published	2026-06-05T10:50:15
Discovery Source	Rss

Executive Summary

Over 900 internet-exposed automatic tank gauge (ATG) systems at US gas stations and critical infrastructure sites show evidence of active exploitation by threat actors. Attackers are exploiting hardcoded credentials, authentication bypasses, and command injection flaws to modify fuel monitoring configurations, capabilities that can disable leak detection and cause physical equipment damage. Security researchers confirm attacks are ongoing, elevating the threat to critical infrastructure safety and environmental compliance.

Technical Analysis

External scans identify 1,061 globally exposed ATG IPs, with 909 in the United States (data sourced from third-party exposure scanning). Affected vendors include Franklin Fueling, Veeder-Root, and OPW. The attack surface is entirely network-accessible, systems are directly internet-exposed with no adequate access controls. Exploitation chains leverage five weakness classes: CWE-798 (hardcoded credentials), CWE-287 (authentication bypass), CWE-78 (OS command injection), CWE-89 (SQL injection), and CWE-269 (improper privilege management). No single CVE identifier or vendor-issued patch IDs are currently available in the source data; remediation centers on network isolation and credential remediation until vendor patches are released. MITRE ATT&CK techniques observed include T1190 (Exploit Public-Facing Application), T1078.001 (Valid Accounts: Default Accounts), T1059 (Command and Scripting Interpreter), T1548 (Abuse Elevation Control Mechanism), T1562/T1562.001 (Impair Defenses/Disable or Modify Tools), T0831 (Manipulation of Control), T0810 (Damage to Property), T0816 (Device Restart/Shutdown), and T0812 (Default Credentials). Successful

exploitation enables configuration modification of tank overfill protection and leak detection thresholds, creating physical safety and environmental hazard beyond data loss.

Action Checklist

1. Step 1: Containment. Immediately remove ATG systems (Franklin Fueling, Veeder-Root, OPW) from direct internet exposure. Place all ATG management interfaces behind a firewall with explicit deny-all inbound rules. If remote access is operationally required, restrict to VPN with MFA only (NIST AC-17, CIS 6.4). Run a Shodan or similar external exposure verification tool scoped to your organization's IP ranges to confirm no ATG interfaces are internet-reachable.
2. Step 2: Detection. Query firewall and network flow logs for inbound connections to ATG management ports (typically TCP 10001, 502 Modbus, and vendor-specific web UI ports). Review authentication logs on all ATG systems for failed login attempts, successful logins from external IPs, and configuration change events. Check for command execution patterns consistent with T1059 and T1548. If SIEM coverage exists, alert on any external source IP authenticating to ICS/SCADA assets (NIST AU-6, CIS 8.2).
3. Step 3: Eradication. Change all default and hardcoded credentials on ATG systems immediately; disable any accounts with vendor-default passwords (CIS 4.7, CIS 5.2, NIST AC-2). Contact Franklin Fueling, Veeder-Root, and OPW directly for vendor-specific firmware updates addressing CWE-798, CWE-287, CWE-78, CWE-89, and CWE-269. Apply vendor patches as released. Where firmware updates are unavailable, document the gap and apply compensating network controls.
4. Step 4: Recovery. After isolation and credential rotation, verify ATG systems are functioning within normal operational parameters, confirm leak detection thresholds, overfill protection settings, and alarm configurations have not been modified. Establish a baseline configuration snapshot and monitor for deviation (NIST CM controls, D3-SFA: System File Analysis). Restore operations only after confirming no attacker persistence in system configuration.
5. Step 5: Post-Incident. Conduct an asset inventory audit to confirm all OT/ICS assets are identified and their network exposure documented (CIS 1.1, NIST AC-20). Formalize a process for periodic external exposure checks on ICS assets. Review whether OT systems are included in your vulnerability management program (CIS 7.1). Implement network segmentation separating ATG systems from IT networks and the internet as a permanent architectural control (NIST AC-4, NIST SC controls).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISA (report at cisa.gov/report) and senior leadership if: any ATG unit's leak detection threshold was confirmed modified or disabled during the compromise window (EPA notification obligation), if Iranian-linked threat actor IOCs are confirmed in your environment matching the joint CISA/FBI/NSA/DOE advisory, if any ATG unit is unresponsive to configuration verification commands post-isolation (indicating possible firmware-level persistence), or if your organization lacks the capability to verify ATG configuration integrity within 4 hours of this advisory.

Recovery Notes	Before returning any ATG system to operational monitoring duty, independently verify all leak detection, overfill protection, and high-product alarm thresholds against your jurisdiction's EPA-mandated values and the vendor's factory configuration documentation — do not rely solely on the system's self-reported status, as CWE-78 command injection and CWE-269 privilege escalation could allow an attacker to spoof reported values. Monitor ATG configuration exports via automated weekly diff for a minimum of 90 days post-recovery, given that this campaign reflects sustained, active targeting of US fuel infrastructure rather than opportunistic scanning. If any configuration parameter cannot be verified as unmodified, treat the unit as compromised and escalate to the vendor for a full firmware re-flash before restoring EPA-reportable leak detection coverage.
Forensic Artifacts	ATG system internal event/audit log exports (Veeder-Root TLS series: retrievable via serial command 'I20200'; Franklin Fueling TS-series: diagnostic menu export) — these record configuration change events with timestamps and, on networked units, the source IP of the modifying session, directly evidencing attacker modification of leak detection or alarm parameters. | Modbus/TCP session transcripts (TCP 502) captured via Wireshark/tshark or Zeek on the OT network tap — function code 0x10 (Write Multiple Registers) and 0x05/0x0F (Write Coil/Multiple Coils) packets from non-RFC1918 source IPs are the network-level forensic signature of remote configuration tampering on Veeder-Root and compatible ATG units. | Firewall and router connection logs for TCP 10001 (Franklin Fueling ATG proprietary protocol), TCP 502 (Modbus), and vendor web UI ports (TCP 80/443) — session records with external source IPs, byte counts, and duration establish the attacker dwell time and scope of access prior to containment. | Serial-to-IP converter session logs (Moxa NPort, Digi Connect series) placed in front of ATG units — these devices often retain session establishment logs independent of the ATG itself and may capture attacker authentication attempts exploiting CWE-287 (authentication bypass) that the ATG unit does not natively log. | Pre- and post-compromise ATG configuration exports (tank parameters, alarm thresholds, network settings, user account list) as structured diffs — the delta between a known-good baseline and the attacker-modified state constitutes direct forensic evidence of sabotage intent, required for both CISA incident reporting and any EPA regulatory notification triggered by confirmed leak detection disablement.

Per-Action IR Details

Step 1: Containment — Immediately remove ATG systems (Franklin Fueling, Veeder-Root, OPW) from direct internet exposure. Place all ATG management interfaces behind a firewall with explicit deny-all inbound rules. If remote access is operationally required, restrict to VPN with MFA only (NIST AC-17, CIS 6.4). Run a Shadowserver or Shodan query against your organization's IP space to confirm no ATG interfaces are internet-reachable.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 6.4 (Require MFA for Remote Network Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use the host-based Windows Firewall (netsh advfirewall) or iptables/nftables on Linux-based ATG gateways to block inbound TCP 10001, TCP 502, and any vendor web UI ports (e.g., TCP 80/443 on Franklin Fueling TS-550/TS-5000 or Veeder-Root TLS-350/450 serial-to-IP adapters). Confirm internet exposure with a free Shodan CLI query: 'shodan search --fields ip_str,port,org "Franklin Fueling" OR "Veeder-Root" OR "TLS-350" country:US'. Run weekly via cron to detect re-exposure. A 2-person team can complete ACL changes and Shodan verification in under 2 hours.

Evidence: Before isolating, capture full netflow or pcap from the ATG-facing network segment using Wireshark (tshark -i -w atg_pre_isolation.pcap -f 'tcp port 10001 or tcp port 502') to preserve attacker session data. Export firewall connection-state tables showing all active and recent inbound sessions to ATG management IPs. Screenshot or export any Shodan/Shadowserver results confirming pre-isolation exposure. Preserve router/switch ARP tables and MAC address logs to identify attacker pivot points within the OT network.

Step 2: Detection — Query firewall and network flow logs for inbound connections to ATG management ports (typically TCP 10001, 502 Modbus, and vendor-specific web UI ports). Review authentication logs on all ATG systems for failed login attempts, successful logins from external IPs, and configuration change events. Check for command execution patterns consistent with T1059 and T1548. If SIEM coverage exists, alert on any external source IP authenticating to ICS/SCADA assets (NIST AU-6, CIS 8.2).

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 against exported ATG system logs and firewall syslogs: grep -E '(10\.0\.0\.|external_ip_range)' /var/log/atg/access.log to surface non-RFC1918 source IPs. For Veeder-Root TLS systems, pull the audit trail via the serial/IP interface using a terminal emulator (e.g., PuTTY) and the 'I20200' function code to retrieve event logs. For Franklin Fueling TS-series, export the diagnostic log via the web UI and grep for configuration change entries. Use Zeek (formerly Bro) on a network tap to parse Modbus/TCP TCP 502 traffic and flag write-register commands (function code 0x10) originating from non-local IPs — these indicate active configuration tampering consistent with MITRE ATT&CK T1548 abuse on ICS devices. Cross-reference source IPs against CISA's published Iranian-linked threat actor IOC lists from the joint advisory.

Evidence: Preserve ATG system-internal event logs before any credential changes — these logs record configuration modifications with timestamps and, on some Veeder-Root TLS-450 units, the source IP of the session. Capture full Modbus/TCP session transcripts (TCP 502) from network taps; attacker writes to holding registers (FC 16) or coil outputs (FC 5/15) targeting leak detection thresholds or alarm setpoints are the forensic signature of this campaign. Export firewall deny/allow logs for TCP 10001 and TCP 502 covering at minimum the prior 90 days. Capture authentication logs from any serial-to-IP converter (e.g., Moxa, Digi) sitting in front of the ATG unit, as these may log session establishment even when the ATG itself does not.

Step 3: Eradication — Change all default and hardcoded credentials on ATG systems immediately; disable any accounts with vendor-default passwords (CIS 4.7, CIS 5.2, NIST AC-2). Contact Franklin Fueling, Veeder-Root, and OPW directly for vendor-specific firmware updates addressing CWE-798, CWE-287, CWE-78, CWE-89, and CWE-269. Apply vendor patches as released. Where firmware updates are unavailable, document the gap and apply compensating network controls.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Vendor firmware update contacts: Franklin Fueling Systems support at +1-800-984-6737 or fuelingsystems.com/support; Veeder-Root at veeder.com/support; OPW at opwglobal.com. Request explicit patch status for CWE-798 (hardcoded credentials), CWE-287 (authentication bypass), CWE-78 (OS command injection), CWE-89 (SQL injection), and CWE-269 (privilege escalation) for your specific model and firmware version. Where no patch exists, document the open gap in your risk register with a compensating control entry: ACL blocking all inbound to ATG ports plus a manual weekly review of ATG configuration exports to detect unauthorized changes. Use a diff tool (diff or fc) to compare weekly configuration exports against a known-good baseline.

Evidence: Before changing credentials, document all existing account names, privilege levels, and last-login timestamps on each ATG unit — this establishes whether attackers created persistence accounts, which is a known TTPs for Iranian-linked ICS intrusions. If the ATG supports firmware version queries, record the current firmware string

verbatim; this is required for vendor patch applicability confirmation and for any regulatory incident report. Photograph or screenshot physical unit serial numbers and model designations for the vendor patch inquiry. Preserve a read-only configuration export (tank parameters, alarm thresholds, network settings) from each unit before credential rotation to document the attacker-modified state as forensic evidence.

Step 4: Recovery — After isolation and credential rotation, verify ATG systems are functioning within normal operational parameters — confirm leak detection thresholds, overfill protection settings, and alarm configurations have not been modified. Establish a baseline configuration snapshot and monitor for deviation (NIST CM controls, D3-SFA: System File Analysis). Restore operations only after confirming no attacker persistence in system configuration.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-11 (Audit Record Retention), NIST AU-9 (Protection Of Audit Information), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Export a full configuration dump from each ATG unit (Franklin Fueling: use the TS-series diagnostic menu; Veeder-Root: use the TLS Setup Report printout or serial command 'I20100' for system setup data) and store it as a signed, dated baseline in a write-protected network share or offline media. Compare against vendor-published factory default threshold values for leak detection (typically 0.1 gal/hr for EPA Tier 1) and overfill alarm setpoints to verify attacker modifications have been reverted. Schedule weekly automated config exports via a Python script using pyserial against the ATG serial-to-IP interface and diff against baseline — alert on any delta. A 2-person team can validate all critical parameters (leak detection, overfill, high/low product alarms) against operator logs in 1-2 hours per site.

Evidence: Retain the pre-recovery attacker-modified configuration export as a forensic artifact — this documents exactly which parameters were changed, which is required for EPA/state environmental agency notification if leak detection was disabled during the compromise window. Capture a timestamped configuration export immediately post-recovery as the new baseline. If any leak detection disable period can be confirmed from audit logs, document the exact window for regulatory disclosure purposes. Preserve all network pcap and log evidence under litigation hold given the involvement of Iranian-linked threat actors and potential CISA/FBI reporting obligations.

Step 5: Post-Incident — Conduct an asset inventory audit to confirm all OT/ICS assets are identified and their network exposure documented (CIS 1.1, NIST AC-20). Formalize a process for periodic external exposure checks on ICS assets. Review whether OT systems are included in your vulnerability management program (CIS 7.1). Implement network segmentation separating ATG systems from IT networks and the internet as a permanent architectural control (NIST AC-4, NIST SC controls).

NIST Phase: Post Incident

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 1.2 (Address Unauthorized Assets), 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), NIST AC-20 (Use Of External Systems), NIST AC-4 (Information Flow Enforcement)

Compensating: Use Nmap with the script 'nmap -sV -p 10001,502,80,443,23 --script modbus-discover ' to enumerate all ATG-responsive hosts and verify none are reachable from the IT VLAN or internet egress path. For ongoing exposure monitoring without a commercial ASM tool, configure a monthly cron job running Shodan CLI against your registered IP ranges with keywords specific to your ATG vendor models. Submit your OT asset list to CISA's free Vulnerability Scanning service (cisa.gov/cyber-hygiene-services) for ongoing external exposure monitoring. Document all ATG models, firmware versions, and open CWEs in a simple spreadsheet risk register reviewed quarterly against new vendor advisories.

Evidence: Produce a post-incident lessons-learned report documenting the initial exposure window (date ATG first appeared internet-reachable vs. date discovered), the attack timeline reconstructed from firewall and ATG logs, and any configuration changes confirmed as attacker-made — this report is the basis for CISA voluntary incident reporting under CIRCIA and any applicable state environmental or critical infrastructure notification requirements. Archive all

forensic artifacts (pcaps, log exports, configuration diffs, credential audit outputs) for a minimum of 3 years given the critical infrastructure and potential regulatory dimensions of this incident.

Detection Guidance

Primary detection method: external exposure verification. Run a Shodan or similar external exposure tool scoped to your organization's IP ranges, searching for ATG-specific banners (e.g., 'TLS-450', 'SiteSentinel', 'Veeder-Root', 'Franklin Fueling') or open ports commonly used by ATG systems (TCP 10001, TCP 502, TCP 80/443 on ICS subnets). Any result is a confirmed finding requiring immediate action.

Network log indicators: inbound connections from external IPs to ATG management interfaces; authentication attempts against ATG systems from non-management source IPs; configuration change events in ATG audit logs outside of scheduled maintenance windows.

Behavioral indicators mapped to MITRE techniques: unexpected process execution on ATG hosts (T1059); modification of alarm or threshold configuration files (T0831, D3-SFA); disabling of monitoring or logging functions (T1562.001); use of default or hardcoded credentials in authentication logs (T1078.001, T0812).

Log sources to query: firewall deny/allow logs for ICS network segments; ATG vendor management software audit logs; SIEM alerts for ICS asset authentication events; network flow data on OT VLAN segments.

Note: No specific IOCs (IP addresses, hashes, domains) are confirmed in the available source data. Detection should rely on behavioral and configuration indicators rather than signature-based IOC matching at this time. Monitor threat intelligence sources for released IOC sets as investigations develop.

Indicators of Compromise

Type	Value	Context	Confidence
IP	`No confirmed IOCs available in current source data`	CISA and joint advisory IOC sets not yet published in available sources — monitor CISA advisories at cisa.gov for releases	LOW

Framework Mappings

MITRE-ATTACK

- **T1548** — Abuse Elevation Control Mechanism
- **T1562** — Impair Defenses
- **T1059** — Command and Scripting Interpreter
- **T0831** — Manipulation of Control
- **T0810**
- **T1190** — Exploit Public-Facing Application
- **T0816** — Device Restart/Shutdown
- **T1078.001** — Default Accounts
- **T1562.001** — Disable or Modify Tools

- **T0812** — Default Credentials

NIST-800-53R5

- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **AU-9** — Protection of Audit Information
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **IA-5** — Authenticator Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **2.5** — Allowlist Authorized Software
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.5.23** — Information security for use of cloud services

SOC2-TSC

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

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

HIPAA-SECURITY

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

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1562	Impair Defenses	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T0831	Manipulation of Control	Impact
T0810		
T1190	Exploit Public-Facing Application	Initial-Access
T0816	Device Restart/Shutdown	Inhibit-Response-Function
T1078.001	Default Accounts	Defense-Evasion
T1562.001	Disable or Modify Tools	Defense-Evasion
T0812	Default Credentials	Lateral-Movement

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/over-900-us-gas-stat...	T3
	https://www.bleepingcomputer.com/news/security/over-900-us-gas-stat...	T3
	https://www.bleepingcomputer.com/news/security/european-commission-...	T3
	https://www.bleepingcomputer.com/news/microsoft/microsoft-edge-to-s...	T3
Critical Vulnerabilities Discovered in Automated Tank Gauge Systems	https://www.bitsight.com/blog/critical-vulnerabilities-discovered-a...	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 2026-06-05 19:18 UTC by TJS Security Command Center