MAGNET S2

INTELLIGENCE REPORT

DTG: 260711-1600Z | Geographic Focus: United States (multi-state)

www.magnethf.com

REPORT IDENTIFICATION

Subject	Suspected Iranian Cyber Intrusions Targeting Internet-Exposed Automatic Tank Gauge (ATG) Systems at U.S. Fuel Retail Sites
Purpose	Provide an intelligence assessment of suspected Iranian exploitation of internet-exposed ATG systems monitoring U.S. fuel storage tanks, and relay associated federal mitigation guidance.
DTG	260711-1600Z
Reporting Period	15 May – 11 July 2026
Geographic Focus	United States (multi-state) – Cybersecurity Technology (OT) / Automatic Tank Gauge (ATG) Systems Supporting Fuel Infrastructure
Precedence	RR – PRIORITY
MagCon Status	L3 – ELEVATED (NO CHANGE)
Sources	Multiple source reporting from Local, National, and International platforms. See source list.

SUMMARY (BLUF)

U.S. officials suspect Iranian-linked hackers breached internet-exposed automatic tank gauge (ATG) systems monitoring fuel storage tanks at gas stations across multiple U.S. states, altering operator-facing display readings on devices left online without password protection; no physical damage or altered fuel levels have been confirmed.

The U.S. government has not formally attributed this activity to Iran or any specific actor, citing limited forensic evidence, though Iran's history of targeting similar systems makes it a plausible suspect.

A joint federal advisory issued 2 June 2026 by CISA, FBI, NSA, DOE, EPA, TSA, DOT, and USDA confirms broader, ongoing exploitation of internet-exposed ATG systems nationwide, and open-source scanning has since identified 909 U.S.-based ATG devices still exposed to the public internet.

This activity is assessed as likely consistent with a broader pattern of Iranian-linked targeting of exposed U.S. operational technology (OT) amid the ongoing U.S.-Israel-Iran conflict, though it may equally reflect opportunistic exploitation of a long-known, widespread vulnerability class.

BACKGROUND

Automatic tank gauge (ATG) systems are electronic monitoring devices used to remotely track fuel and liquid levels, temperature, water intrusion, and leak/overfill conditions in storage tanks. They are widely deployed at gas stations and across the Energy, Chemical, Food and Agriculture, and Transportation Systems sectors, and to a lesser extent in the water sector.

Industry estimates place the number of fuel retail sites using ATG systems at roughly 148,000 across North America. Many ATG units were originally designed for isolated, dial-up-era remote access and were not built to be internet-facing; a substantial number nonetheless remain reachable from the public internet, frequently over default TCP ports 8001, 9001, or 10001.

Internet exposure of ATG systems is a long-documented vulnerability class rather than a newly discovered one. Security researchers (Rapid7) identified more than 5,800 internet-exposed ATGs in 2015, and follow-on vulnerability research (Bitsight, September 2024) identified additional critical vulnerabilities across multiple ATG manufacturers' products.

This incident occurs against the backdrop of an active U.S.-Israel-Iran military conflict and a documented pattern of Iranian-linked cyber activity against U.S. critical infrastructure, including a separate joint advisory (April 2026) linking Iranian state-backed actors to attacks on Rockwell Automation/Allen-Bradley programmable logic controllers (PLCs) since March 2026 that caused financial losses and operational disruption. CSIS's Significant Cyber Incidents timeline separately documents a long-running pattern of Iranian and Iran-linked cyber operations against gas, energy, and other critical infrastructure targets.

SITUATION

Timeline

2026-05-15	CNN reports U.S. officials suspect Iranian hackers are behind breaches of ATG systems monitoring fuel tanks at gas stations across multiple states; systems were internet-exposed and lacked password protection. Attackers could alter display readings but not actual fuel levels. No physical damage confirmed.
2026-05-15/16	Follow-on coverage (Newsweek, Cybernews, WION, Raw Story, Security Magazine) reiterates CNN reporting; officials caution attribution may not be conclusively confirmed due to limited forensic evidence.
2026-06-02	CISA, FBI, NSA, DOE, EPA, TSA, DOT, and USDA jointly release a fact sheet, "CISA and Partners Urge Hardening Automatic Tank Gauge Systems," warning of ongoing compromise of internet-exposed ATG systems via command execution. The advisory does not attribute activity to a specific nation-state or group.
2026-06-03	NSA issues a press release affirming its co-authorship of the ATG hardening guidance.
2026-06-04/05	Trade press (Industrial Cyber, BleepingComputer) reports on the advisory; Shadowserver scanning identifies 1,061 internet-exposed ATG IP addresses globally, 909 of which are in the United States (port 10001/tcp), after excluding suspected honeypots.

Reported Tactics, Techniques, and Procedures (TTPs)

- Authentication bypass and use of hardcoded or default credentials to gain unauthorized access to ATG management interfaces.
- OS command execution and SQL injection used to run arbitrary code and manipulate underlying device databases.
- Privilege escalation to obtain full administrator control of the ATG device, equivalent to physical console access.
- Manipulation of operator-facing display readings and, per CISA, potential ability to disable system alarms and alter tank labels or alarm thresholds.

Scope of Exposure

Shadowserver identified 1,061 internet-exposed ATG IP addresses globally as of 5 June 2026 (port 10001/tcp), with 909 located in the United States, after excluding devices assessed to be honeypots. The federal joint advisory does not attribute the underlying malicious activity to a specific nation-state or threat actor group.

COMMENTS / ASSESSMENT

MAGNET S2 assesses that the May 2026 ATG intrusions likely reflect the same category of low-sophistication, opportunistic exploitation of internet-facing OT devices that has been documented against U.S. and allied infrastructure for over a decade, rather than a bespoke or highly targeted operation. The technique — exploiting devices with no or default credentials — requires minimal capability and is consistent with mass-scanning tradecraft

rather than a tailored intrusion chain.

Attribution to Iran is plausible given Tehran's documented history of targeting fuel and gas-related monitoring systems, and Iranian-linked actors' demonstrated willingness to strike low-profile U.S. critical infrastructure that sits outside the reach of conventional military options. However, this assessment should be treated as suggestive rather than confirmed: the U.S. government's own joint advisory pointedly declines to attribute the broader ATG exploitation activity to any actor, and officials briefed on the original incident indicated that limited forensic evidence may prevent definitive attribution.

The gap between the number of confirmed-affected sites (undisclosed, but described as "multiple states") and the number of currently exposed devices (909 in the U.S. alone) indicates the addressable attack surface is significantly larger than the disclosed incident count, and further opportunistic compromise attempts should be expected absent broad remediation.

Probability Assessment

ASSESSMENT	LIKELIHOOD	RATIONALE
Iranian state-linked or state-tolerated actors conducted the May 2026 ATG intrusions.	LIKELY	Consistent with Iran's documented history of targeting fuel/gas monitoring and OT systems; no forensic confirmation has been publicly disclosed.
Intrusions reflect opportunistic scanning of exposed devices rather than a coordinated, targeted campaign.	LIKELY	Low-sophistication technique (default/no credentials) is consistent with mass scanning behavior documented by Shadowserver and prior researchers since 2015.
Additional unreported ATG compromises exist beyond those already disclosed.	ROUGHLY EVEN	909 U.S. devices remain internet-exposed as of early June per Shadowserver; exposure scope suggests attack surface exceeds confirmed incident count.
Activity could escalate to safety-relevant consequences (e.g., masked fuel leak, disabled alarms).	UNLIKELY / PLAUSIBLE	No physical damage or altered fuel levels confirmed to date; however, CISA assesses compromise could disable alarms and manipulate readings.
U.S. government will formally attribute this activity to Iran.	UNLIKELY NEAR TERM	Joint federal advisory (2 Jun 2026) explicitly declines attribution; officials indicate limited forensic evidence may preclude definitive attribution.

INTELLIGENCE GAPS

- No public forensic attribution linking the May 2026 intrusions to a specific Iranian government entity, unit, or known hacking group.
- Total number of affected gas stations/states, and duration of unauthorized access, has not been disclosed.
- Unknown whether attackers who accessed ATG systems prior to the 2 June advisory retain persistent access following remediation efforts.
- No confirmed reporting on whether any non-fuel-retail ATG deployments (e.g., water sector) have been compromised, as opposed to merely exposed.

MITIGATION RECOMMENDATIONS

- Eliminate public internet exposure of ATG serial ports/interfaces (default TCP 8001, 9001, 10001); if remote access is required, place devices behind a firewall, access control list (ACL), or VPN gateway rather than direct exposure.
- Replace all default or factory-set ATG passwords with long, unique, complex credentials, and implement phishing-resistant multifactor authentication wherever the device/interface supports it.
- Segment back-office and point-of-sale (POS) networks from OT/ATG assets so that a compromise in one system cannot reach fuel-monitoring equipment.

- Work with certified ATG service providers to verify configuration compliance, apply the latest manufacturer firmware/security patches, and confirm no unauthorized settings changes are present.
- Enable logging and actively monitor for exposed device interfaces, unauthorized connections, suspicious alarms, alarm-threshold modifications, and tank-label changes.
- Prepare and rehearse manual gauging and control procedures for use during a network outage or suspected ATG compromise.
- Report suspected ATG-related incidents promptly to CISA (report@cisa.gov / 888-282-0870) and, where relevant, the FBI's Internet Crime Complaint Center (www.ic3.gov).

MAGNET GUIDANCE

- Operators and members with commercial, fabrication, or facility-management ties to fuel retail or storage sites should treat any internet-connected ATG or similar OT monitoring equipment as reportable exposure and confirm with site owners that CISA's hardening guidance has been applied.
- Individual operators: if you manage or advise on any fuel-storage, generator fuel, or bulk-liquid monitoring system with remote/internet connectivity, verify it is not directly internet-facing and that default credentials have been changed.
- Preparedness/emcomm groups: treat potential disruption to fuel retail inventory visibility (not fuel supply itself) as a low-probability, low-current-impact contingency; no operational change to fuel logistics planning is warranted based on current reporting.
- Communications posture: this event does not currently affect PACE (Primary-Alternate-Contingency-Emergency) communications planning. If a future ATG-linked incident causes confirmed fuel-availability disruption at the local level, elevate internal net traffic to the Alternate tier to coordinate resource-sharing and status reporting among group members.
- Continue routine monitoring of CISA/FBI/NSA advisories for updates on attribution or expanded targeting; MAGNET S2 will issue a follow-on report if attribution is confirmed or if physical/safety consequences are reported.

SOURCE LIST

[1] CISA — Joint fact sheet, "CISA and Partners Urge Hardening Automatic Tank Gauge Systems," co-issued with FBI, NSA, DOE, EPA, TSA, DOT, and USDA (2 Jun 2026); outlines TTPs and mitigations, declines attribution. [A1]

[2] CISA — Press Release — "CISA Urges Stronger Security for Automatic Tank Gauge Systems," summarizing the joint fact sheet and quoting Acting Director Nick Andersen. [A1]

[3] National Security Agency — Press release confirming NSA's co-authorship of the joint ATG hardening guidance (3 Jun 2026). [A1]

[4] CNN — Original reporting (15 May 2026) that U.S. officials suspect Iranian hackers breached ATG systems at gas stations in multiple states. [B2]

[5] BleepingComputer — "Over 900 US gas station tank gauge systems exposed to attacks," reporting Shadowserver scan results (5 Jun 2026). [B2]

[6] BleepingComputer — "CISA warns of cyberattacks targeting fuel tank monitoring systems," summarizing the 2 Jun 2026 joint advisory. [B2]

[7] Industrial Cyber — Coverage of the joint advisory and CISA statement, with context on the preceding May incident. [B2]

[8] WaterISAC — TLP:CLEAR bulletin summarizing the CISA advisory with sector-specific analyst notes for water/wastewater utilities. [B2]

[9] CGI United States (blog) — Industry commentary on ATG exposure scale (~148,000 North American fuel retail sites) and operator risk-management practice. [C3]

[10] Dark Reading — "Fuel Tank Breaches Expand Scope of Iran's Cyber Offensive," with security-industry commentary on OT exposure risk. [B2]

[11] Newsweek — Follow-on reporting on the suspected Iranian ATG breach, including CISA mitigation guidance and historical Iranian ICS-targeting context. [B3]

[12] Security Magazine — Industry-expert reaction roundtable on the suspected Iranian ATG breach and its OT/IT convergence implications. [B3]

[13] CSIS — “Significant Cyber Incidents” timeline (living document), providing long-term context on Iranian and Iran-linked cyber operations against critical infrastructure. [A1]

Submit reports through established MAGNET situational awareness channels.
To Learn More About MAGNET, Visit www.MAGNETHF.COM