June 2, 2026

CISA and Partners Urge Hardening Automatic Tank Gauge Systems

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Department of Energy (DOE), the Environmental Protection Agency (EPA), the Transportation Security Administration (TSA), the Department of Transportation (DOT), and the U.S. Department of Agriculture (USDA)—hereafter referred to as "the authoring organizations"—are aware of malicious cyber activity targeting U.S.-based automatic tank gauge (ATG) systems. ATG systems are widely used throughout the Energy, Chemical, Food and Agriculture, and Transportation Systems Sectors for automated and remote monitoring of storage tank parameters, including fuel and liquid levels, temperature, and possible leak detection. The authoring organizations urge ATG owners and operators to defend against this malicious activity by securing their ATG systems with strong passwords and by removing them from the internet to reduce public exposure.

Threat

The recent malicious cyber activity observed by the authoring organizations—which the U.S. government has not yet attributed to a nation-state or threat actor group—involves cyber threat actors compromising internet-exposed ATG systems and subsequently modifying them through command execution. This fact sheet provides insight into probable tactics, techniques, and procedures (TTPs) leveraged by these cyber actors, highlights risk factors associated with such compromises, and provides mitigation guidance and resources to reduce the likelihood of continued malicious activity targeting U.S.-based ATG systems.

Cyber threat actors may exploit flaws in ATG systems through multiple attack vectors:

- **Authentication Bypass and Hardcoded Credentials**: Threat actors gain unauthorized access to device management interfaces.
- **OS Command Execution and Structured Query Language (SQL) Injection**: Threat actors execute arbitrary code and manipulate underlying databases.
- **Privilege Escalation**: Threat actors achieve full administrator privileges over the device application and operating system.

Should a cyber threat actor exploit these vulnerabilities and compromise an ATG system, they could disrupt or manipulate the below critical functions by interfacing directly with the tank management as though they possessed legitimate physical access to the system console. The cyber threat actors could:

- **Alter system(s) attributes**, such as network settings, product identifiers, tank volumes, and pump controls;
- **Compound operational malfunctions**; components operating incorrectly could create a denial of view condition of tank fill levels, which could cause permanent damage to the tank system's critical function;
- **Disable system alerts**, reducing an operator's ability to detect and mitigate system issues increases the risk of environmental or physical hazards from incidents such as leaks or relay failures.

Mitigations

The authoring organizations recommend ATG owners immediately implement the following recommendations:

1. **Eliminate public internet exposure: Do not expose the ATG serial port (e.g., default TCP port 8001, 9001, or 10001), or other applicable web interfaces, directly to the internet**. If remote access to the port is necessary, consider the following options:
    a. **Restrict access:** Use a firewall, access control list (ACL), or virtual private network (VPN) to restrict access.
2. **Enforce Credential Security: Change any default passwords immediately** [CPG 3.A] and implement strong, unique security codes and administrative credentials for all interfaces, including the serial port. Further, implement phishing-resistant multifactor authentication wherever feasible [CPG 3.F]. If unfamiliar with these procedures, contact your ATG service provider for assistance.
3. **Apply Patches**: Where possible, work with certified ATG service providers, if available, to verify compliance, update software, and apply the latest security patches from the manufacturer.
4. **Monitor and Report**: Organizations should actively monitor networks for unauthorized access.
    a. **Enable logging and audit and monitor logs** to identify exposures of ATG device interfaces, unauthorized connections, suspicious alarms, alarm threshold modifications, tank label changes, and other system modifications [CPG 3.Q].
    b. **Report suspected incidents** promptly to the CISA portal.
5. **Engage your third-party service providers** to adopt CISA, FBI, EPA, and DOE's Primary Mitigations to Reduce Cyber Threats to Operational Technology [CPG 1.E].

Resources

The authoring organizations recommend ATG owners and operators review the following resources and implement suggested mitigations, where possible, to enhance their security posture.

1. For more information on mitigating cyber threat activity targeting internet-exposed OT and ICS, see CISA, FBI, EPA, and DOE's Primary Mitigations to Reduce Cyber Threats to Operational Technology fact sheet.
2. For more information on vulnerabilities affecting ATG systems, see Critical Vulnerabilities Discovered in Automated Tank Gauge Systems.[i]
3. For ways to identify and remove internet-accessible assets, see CISA's Internet Exposure Reduction Guidance web page.
4. For more information about how organizations should design, secure, and manage connectivity in OT, see Secure connectivity principles for Operational Technology (OT).

Contact Information

The authoring organizations recommend U.S. organizations report suspicious or criminal activity related to information provided in this fact sheet.

- **CISA:** Contact CISA's 24/7 Operations Center via report@cisa.gov or 888-282-0870.
  - When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
  - For more information on reporting a cyber incident, refer to CISA's Voluntary Cyber Incident Reporting web page.
- **FBI:** File a complaint with the Internet Crime Complaint Center (IC3) at www.ic3.gov. When available, include the following incident information: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting organization; and designated point of contact.
- **EPA**: Contact EPA's Office of National Security via ONS-OC@epa.gov.
- **DOE:** Entities required to report incidents to DOE should follow established reporting requirements, as appropriate. For other energy sector inquiries, contact EnergySRMA@hq.doe.gov.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by the authoring organizations.

[i] Pedro Umbelino, "Critical Vulnerabilities Discovered in Automated Tank Gauge Systems," *Bitsight,* October 11, 2023, bitsight.com/blog/critical-vulnerabilities-discovered-automated-tank-gauge-systems.