TLP AMBER – *Limited disclosure, restricted to participants' organization and its clients.*

Automatic Tank Gauge Manipulation by Malicious Cyber Threat Actors

April 27, 2026

The Energy Threat Analysis Center (ETAC) is aware of multiple recent incidents of malicious cyber threat actors manipulating automatic tank gauges (ATG). On or around March 8, 2026, an unattributed cyber threat actor targeted and obtained access to internet-connected ATGs at locations in the United States. All ATGs accessed were found to expose TCP port 10001, the default serial port, at the time of the reported exploitation. Based on information received and assessed by a supporting organization, it appears that no security code(s) or password(s) were set on the devices, allowing the cyber threat actor to execute various commands and modify the ATG alarm levels.

ETAC is aware of multiple publicly available tools and articles that make this exploitation trivial. Based on these findings, ETAC recommends that ATG owners implement the following recommendations:

1. Do not directly expose the ATG serial port (default TCP port 10001) or any other applicable web interfaces on the device to the internet. If remote access to the serial port is required, consider the following options:
    a. Use a firewall, an access control list, or a VPN to limit access to the port.
    b. Require a security code or password to access the serial port.
2. Audit and monitor logs to identify exposures of ATG device interfaces, unauthorized connections, suspicious alarms, modifications to alarm thresholds, tank label changes, and other system changes.

For additional mitigation guidance, please see the U.S. Department of Energy's "Primary Mitigations to Reduce Cyber Threats to Operational Technology": https://www.cisa.gov/sites/default/files/2025-05/fact-sheet-primary-mitigations-to-reduce-cyber-threats-to-operational-technology-508c.pdf.

> *Mitigations, recommendations, TTPs, and indicators are not comprehensive and might not be applicable to your network's configuration. The ETAC recommends these actions because they are broadly effective against these threats and work in most environments. Suggested scripts and rules must be tailored for your environment.*

Examples of code used to interact with an exposed ATG: https://github.com/eredden/Veeder-Root-TLS-Client/tree/main and https://dk27ss.github.io/writeups/atg-gas-stations-exploit/.

ETAC encourages readers to report anomalous or malicious activity to their appropriate ISAC, CISA, or the FBI.

- E-ISAC: operations@eisac.com
- DNG-ISAC: analyst@dngisac.com
- ONE-ISAC: soc@oneisac.org
- CISA: Incident Reporting System
- FBI: Internet Crime Complaint Center

ETAC welcomes feedback and questions. There are several ways to reach us.

- Rate this report in the E-ISAC portal
- Email the E-ISAC Watch at operations@eisac.com
- Email the ETAC at etac@hq.doe.gov