مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

# Critical Vulnerabilities in Automated Tank Gauge (ATG) Systems

Tracking #:432316328

Date:25-09-2024



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that recent findings have revealed critical vulnerabilities in Automated Tank Gauge (ATG) systems, which are widely used for monitoring fuel storage across various sectors.

## TECHNICAL DETAILS:

Bitsight has identified several critical vulnerabilities within commonly used automated tank gauge (ATG) systems. These vulnerabilities could potentially compromise the integrity and safety of storage tank operations, leading to unauthorized access, data manipulation, and physical damage. Affected systems are widely used across various industries, including oil and gas, chemical manufacturing, and water treatment.

**Key Findings:**

- Vulnerability Discovery: Bitsight TRACE identified multiple critical 0-day vulnerabilities across six ATG systems from five different vendors. These vulnerabilities allow attackers to gain full control over the ATG systems, which could lead to disastrous consequences if abused.
- Historical Context: ATGs have been flagged as vulnerable since at least 2015, with thousands of devices exposed to the internet without proper security measures. Despite past warnings, many ATGs remain online and accessible.
- Potential Exploits: The vulnerabilities could enable attackers to change tank information, resize tanks fraudulently, shut down dispensing operations, capture sensitive corporate data, and even disrupt critical operations in hospitals and emergency services.

**Vulnerability Details:**

| PRODUCT | VULNERABILITY TYPE | CVE | CVSS 3.1 |
|---|---|---|---|
| Maglink LX | OS Command Injection | CVE-2024-45066 | 10 |
| Maglink LX | OS Command Injection | CVE-2024-43693 | 10 |
| Maglink LX4 | Hardcoded credentials | CVE-2024-43423 | 9.8 |
| OPW SiteSentinel | Authentication Bypass | CVE-2024-8310 | 9.8 |
| Proteus® OEL8000 | Authentication Bypass | CVE-2024-6981 | 9.8 |
| Maglink LX | Authentication Bypass | CVE-2024-43692 | 9.8 |
| Alisonic Sibylla | SQL Injection | CVE-2024-8630 | 9.4 |
| Maglink LX | XSS | CVE-2024-41725 | 8.8 |
| Maglink LX4 | Privilege Escalation | CVE-2024-45373 | 8.8 |
| Franklin TS-550 | Arbitrary File Read | CVE-2024-8497 | 7.5 |

## RECOMMENDATIONS:

- Immediate System Audit: Conduct a thorough audit of all ATG systems to identify potential vulnerabilities.
- Software Updates: Reach out to ATG system vendors for guidance on available patches and updates.

- Conduct Risk Assessment: Perform a comprehensive risk assessment to understand the potential impact of these vulnerabilities on your operations.
- Implement Security Measures: Execute the recommended security measures, including network segmentation, access controls, and enhanced monitoring.
- Train Personnel: Educate staff on the importance of cybersecurity and the specific risks associated with ATG systems.
- Review Incident Response: Update incident response plans to include procedures for addressing potential breaches related to ATG systems.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://www.bitsight.com/blog/critical-vulnerabilities-discovered-automated-tank-gauge-systems