مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerabilities in Veeder-Root Automatic Tank Gauge System

Tracking #:432317861
Date:27-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple critical vulnerabilities affecting the Veeder-Root TLS4B Automatic Tank Gauge (ATG) System, widely used in the energy sector for monitoring and managing fuel storage.

TECHNICAL DETAILS:

These vulnerabilities — Command Injection (CVE-2025-58428) and Integer Overflow or Wraparound (CVE-2025-55067) — can be exploited remotely with low attack complexity. A successful attack could enable remote code execution, full shell access, lateral movement, denial-of-service, and administrative lockout of core system functions.

Veeder-Root has released a security patch (Version 11.A) addressing the command injection vulnerability and is preparing a fix for the integer overflow flaw.

Vulnerability Details

1. **CVE-2025-58428 — Command Injection (CWE-77)**
   - **Severity:** Critical (CVSS v4: 9.4 / CVSS v3.1: 9.9)
   - **Attack Vector:** Network (Remote, Low Complexity, Credentialed)
   - **Affected Versions:** TLS4B versions prior to 11.A
   - **Impact:** Remote Command Execution, Full Shell Access, Lateral Movement
   - **Description:**
     The TLS4B's SOAP-based web service handler improperly neutralizes special elements in user input. Authenticated remote attackers can inject arbitrary commands and gain full control over the system's Linux OS. Successful exploitation can result in remote code execution, full device compromise, and potential network propagation.

2. **CVE-2025-55067 — Integer Overflow or Wraparound (CWE-190)**
   - **Severity:** High (CVSS v4: 7.1 / CVSS v3.1: 7.1)
   - **Attack Vector:** Network (Low Complexity, Credentialed)
   - **Affected Versions:** All TLS4B versions (fix pending)
   - **Impact:** Denial of Service (DoS), System Lockout, Timer Failures
   - **Description:**
     The TLS4B system fails to properly handle Unix time values exceeding the 2038 epoch rollover, resulting in a reset to 1901. This time reset leads to authentication errors, log corruption, and operational failures. An attacker could exploit this flaw by manipulating system time to trigger a DoS condition, disrupting core ATG operations.

Mitigations & Recommendations

- **CVE-2025-58428:**
  Upgrade TLS4B systems to Version 11.A immediately to remediate the command injection flaw.
- **CVE-2025-55067:**
  Await vendor patch. In the interim, adhere to Veeder-Root's network security best practices and restrict system time manipulations.

RECOMMENDATIONS:

- Upgrade the TLS4B system to Version 11.A to fix the command injection flaw, and apply Veeder-Root's network security best practices until the patch for the integer overflow issue is released.
- Isolate ATG systems from business networks, restrict remote access, and use secure VPNs with monitoring to prevent unauthorized command execution or service disruption.

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.veeder.com/us/network-security-reminder
- https://www.cve.org/CVERecord?id=CVE-2025-55067
- https://www.cve.org/CVERecord?id=CVE-2025-58428