مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical SQL Injection Vulnerabilities in Siemens TeleControl Server Basic

Tracking #:432317119

Date:28-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Siemens released security updates to address multiple critical SQL injection vulnerabilities in Siemens TeleControl Server.

TECHNICAL DETAILS:

Multiple critical SQL injection vulnerabilities have been identified in Siemens TeleControl Server Basic software versions prior to V3.1.2.2. These vulnerabilities may allow remote attackers to gain unauthorized access to the system's database, manipulate or exfiltrate sensitive data, cause application crashes, or execute code within an operating system shell using limited service-level privileges.These issues originate from legacy design flaws in SQL handling within the application.
Given the critical CVSS score of 9.8, organizations using TeleControl Server Basic in production—particularly in industrial and critical infrastructure environments—are strongly urged to update immediately and review access to exposed systems.

Detailed Vulnerability Overview:

1. **ICSA-25-112-01: Siemens TeleControl Server Basic SQL**
   - **Description:** Vulnerabilities in the SQL component could allow attackers to execute arbitrary SQL commands, leading to unauthorized data access or manipulation.
   - **Associated CVEs**
     - CVE-2025-27495: CVSS v3.1 score of 9.8, CVSS v4 score of 9.3
     - CVE-2025-27539: CVSS v3.1 score of 9.8, CVSS v4 score of 9.3
     - CVE-2025-27540: CVSS v3.1 score of 9.8, CVSS v4 score of 9.3
     - CVE-2025-29905: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-30002: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-30003: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-30030: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-30031: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-30032: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-31343: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-31349: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-31350: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-31351: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-31352: CVSS v3.1 score of 8.8, CVSS v4 score of 8.7
     - CVE-2025-31353: CVSS v3.1 score of 8.8
   - **Potential Impact:** Data breaches, unauthorized control commands, and system instability.
   - **Affected Products:** TeleControl Server Basic: versions prior to V3.1.2.2
   - **Mitigation:**
     - TeleControl Server Basic: Restrict access to port 8000 on the affected systems to trusted IP addresses only.
     - TeleControl Server Basic: Update to V3.1.2.2 or later version

RECOMMENDATIONS:

- Review and apply the latest patches and firmware updates provided by Siemens.
- Isolate affected systems from untrusted networks until mitigations are in place.

- Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.
- Physically and logically isolate control system networks from the business (IT) network.

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://cert-portal.siemens.com/productcert/pdf/ssa-443402.pdf?ste_sid=56179e4a4121d96c5dc2e4419d469b24