مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Advantech Products

Tracking #:432318238

Date:13-01-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical SQL Injection vulnerability in Advantech products, which could allow unauthenticated attackers to execute SQL commands and potentially compromise sensitive data, system configurations, or control of connected devices.

TECHNICAL DETAILS:

A critical SQL Injection vulnerability has been identified in Advantech's IoT product line. Tracked as CVE-2025-52694 and rated with a CVSS score of 10.0 (Critical), the flaw allows unauthenticated remote attackers to execute arbitrary SQL commands. If exploited, attackers could steal sensitive data, modify system configurations, or gain full control over connected IoT infrastructure.

Vulnerability Details

- **CVE-2025-52694**
- CVSS Score 10.0 Critical
- SQL Injection vulnerability exists in multiple components of Advantech's IoT ecosystem. The flaw allows attackers to send specially crafted SQL commands to the database without authentication. Systems exposed to the Internet are particularly at risk, as attackers do not need valid credentials to exploit the vulnerability.
- Successful exploitation can lead to data compromise, unauthorized configuration changes, and complete control of IoT devices.

Affected Products:

- IoTSuite SaaSComposer: Versions prior to 3.4.15
- IoTSuite Growth Linux docker: Versions prior to V2.0.2
- IoTSuite Starter Linux docker: Versions prior to V2.0.2
- IoT Edge Linux docker: Versions prior to V2.0.2
- IoT Edge Windows: Versions prior to V2.0.2

Fixed Version:

- For IoTSuite SaaSComposer, IoTSuite Growth Linux docker, and IoT Edge Windows, contact Advantech support for the official patched versions.
- For IoTSuite Starter Linux docker and IoT Edge Linux docker, download updates via Advantech's official channels.

RECOMMENDATIONS:

- Apply the latest patches or updated versions without delay.
- Restrict Internet access to IoT management interfaces until systems are updated.
- Monitor network and database activity for signs of SQL Injection attempts or unusual behavior.
- Implement general security best practices, such as strong access controls, network segmentation, and input validation, to reduce the risk of exploitation.

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://nvd.nist.gov/vuln/detail/CVE-2025-52694