مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Advantech WebAccess/SCADA

Tracking #:432318194

Date:30-12-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Advantech WebAccess/SCADA that could be exploited to gain unauthorized access, manipulate system data, or disrupt normal system operations.

TECHNICAL DETAILS:

Multiple security vulnerabilities have been identified in Advantech WebAccess/SCADA. Successful exploitation could allow an authenticated attacker to read, modify, or delete arbitrary files, execute arbitrary SQL commands, or upload malicious files that may lead to remote code execution. These issues pose a significant risk to industrial environments where the affected product is deployed.

Vulnerability Details

- **CVE-2025-14850** – Path Traversal allowing deletion of arbitrary files
  - **CVSS v3.1:** 8.1 (High)
- **CVE-2025-14849** – Unrestricted File Upload allowing remote code execution
  - **CVSS v3.1:** 8.8 (High)
- **CVE-2025-14848** – Absolute Path Traversal allowing file existence disclosure
  - **CVSS v3.1:** 4.3 (Medium)
- **CVE-2025-46268** – SQL Injection allowing execution of arbitrary SQL commands
  - **CVSS v3.1:** 6.3 (Medium)
- **CVE-2025-67653** – Path Traversal allowing file existence disclosure
  - **CVSS v3.1:** 4.3 (Medium)

Collectively, these vulnerabilities could be combined by an attacker to increase their impact, potentially leading to deeper system compromise, expanded unauthorized access, and greater operational disruption within affected environments.

Affected Version

- Advantech WebAccess/SCADA: Version 9.2.1

Fixed Version

- Advantech WebAccess/SCADA 9.2.2 or later

RECOMMENDATIONS:

- Apply vendor-provided patches and updates promptly.
- Restrict access to SCADA systems using strong authentication and role-based access controls.
- Limit network exposure of control system components and avoid direct internet accessibility.
- Monitor systems for unusual activity and review logs regularly.
- Conduct risk assessments before deploying mitigations in production environments.

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.cisa.gov/news-events/ics-advisories/icsa-25-352-06