مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerabilities in AzeoTech DAQFactory

Tracking #:432318206

Date:02-01-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple high-severity vulnerabilities in AzeoTech DAQFactory, which could be exploited through specially crafted files, potentially resulting in information disclosure, application failures, or arbitrary code execution.

TECHNICAL DETAILS:

Multiple high-severity memory corruption vulnerabilities have been identified in AzeoTech DAQFactory. Successful exploitation requires an attacker to load a specially crafted .ctl file, potentially leading to information disclosure, application crashes, or arbitrary code execution in the context of the running process.

High-Severity Vulnerabilities

- **CVE-2025-66590 – Out-of-bounds Write (CWE-787):** May allow memory corruption, system crash, or arbitrary code execution.
- **CVE-2025-66589 – Out-of-bounds Read (CWE-125):** May allow information disclosure or application crash.
- **CVE-2025-66588 – Access of Uninitialized Pointer (CWE-824):** May result in arbitrary code execution.
- **CVE-2025-66586 – Type Confusion (CWE-843):** May lead to memory corruption and code execution.
- **CVE-2025-66585 – Use After Free (CWE-416):** May allow execution of attacker-controlled code.

All vulnerabilities are triggered during parsing of maliciously crafted **.ctl** files.

Affected Versions

- AzeoTech DAQFactory ≤ 20.7 (Build 2555)

Fixed Versions

- AzeoTech DAQFactory 21.1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by AzeoTech.

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-25-345-03