مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in Airleader Master

Tracking #:432318413

Date:17-02-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Airleader Master that could allow malicious file uploads, potentially resulting in remote code execution on the system.

TECHNICAL DETAILS:

A critical vulnerability exists in Airleader Master that allows unauthenticated attackers to upload files without restriction, potentially leading to remote code execution. This vulnerability poses a severe risk to industrial control systems across multiple critical infrastructure sectors, including chemical, energy, healthcare, transportation, and water systems.

Vulnerability Details

- **CVE-2026-1358**
- **CVSS v3.1 Base Score:** 9.8 Critical
- **Vulnerability Type:** Unrestricted Upload of File with Dangerous Type (CWE-434)
- Airleader Master versions **6.381 and earlier** allow unrestricted file uploads to multiple web pages running with maximum privileges. An unauthenticated attacker could exploit this vulnerability to execute arbitrary code on the server.
- **Impact:** Remote code execution, full system compromise

Affected Products

- Product: Airleader Master
- Versions Affected: 6.381 and earlier

Fixed Versions

- Airleader Master version 6.386 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Airleader GmbH.

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-2026-1358?utm_source=feedly