مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Authorization Bypass Vulnerability in Apache NiFi

Tracking #:432318412

Date:17-02-2026

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

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that The Apache Software Foundation has released a security update to address an authorization bypass vulnerability in the Apache NiFi data integration platform.

TECHNICAL DETAILS:

The Apache Software Foundation has released a security update to address a significant vulnerability (CVE-2026-25903) in the Apache NiFi data integration platform. This flaw resides in the framework's authorization logic for "Restricted" components, which are designed to handle sensitive operations or data.

Vulnerability Details:

- **CVE ID-CVE-2026-25903**
- Due to a missing authorization check during the *update* lifecycle phase, a user with lower privileges can modify the configuration properties of a restricted component that was initially added to the flow by a more privileged user. This bypasses the intended security model, allowing unauthorized tampering with sensitive data flows or system-level commands.
- Affected Product: Apache NiFi
- Affected Versions: Apache NiFi (org.apache.nifi:nifi-web-api) 1.1.0 before 2.8.0
- Fixed Version: Apache NiFi 2.8.0

RECOMMENDATIONS:

- Upgrade Apache NiFi immediately to fixed version on all affected deployments.

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.openwall.com/lists/oss-security/2026/02/16/1 /