مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Apache NiFi

Tracking #:432316683

Date:30-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Apache NiFi, a widely used data processing and distribution system. This vulnerability may allow unauthorized users to gain access to sensitive data.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-56512**
- A security vulnerability exists in Apache NiFi. This flaw allows authenticated users with Process Group creation permissions to bypass authorization checks, potentially exposing sensitive data and compromising system security
- **Vulnerability Type:** Missing Complete Authorization for Process Group Creation
- Exploiting this vulnerability could lead to:
  - Unauthorized access to Parameter Contexts
  - Downloading of non-sensitive parameter values
  - Unauthorized use of Controller Services and Parameter Providers
  - Potential data breaches and disruption of critical data pipelines

Affected Versions:

- Apache NiFi 1.10.0 to 2.0.0

Fixed Versions:

- Apache NiFi version 2.1.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-56512