مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerability in Progress Flowmon

Tracking #:432315788
Date:25-04-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Progress Flowmon, a network traffic monitoring and security tool, that could be exploited to gain unauthorized access to affected systems.

## TECHNICAL DETAILS:

**Vulnerability Details:**

- **CVE-2024-2389**
- CVSS Score: 10.0 CRITICAL
- A critical security vulnerability exists in Progress Flowmon, a network traffic monitoring and security tool. This vulnerability allows attackers to remotely access the Flowmon web interface and execute arbitrary commands on the system without any authentication.
- Proof-of-concept exploit code publicly available, increasing the risk of exploitation.

**Impact:**

An attacker can exploit this vulnerability to gain complete control over the affected Flowmon system. This could allow attackers to:

- Steal sensitive data
- Disrupt network operations
- Deploy malware
- Launch further attacks on the network

**Affected Versions:**

Flowmon versions v11.x and v12.x

**Fixed Versions:**

- Flowmon 12.3.5
- Flowmon 11.1.14

## RECOMMENDATIONS:

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

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://support.kemptechnologies.com/hc/en-us/articles/24878235038733-CVE-2024-2389-Flowmon-critical-security-vulnerability