مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in PaperCut

Tracking #:432317549

Date:29-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in PaperCut that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

The vulnerability stems from a CSRF flaw that allows attackers to manipulate system configurations remotely. Under specific conditions, this can escalate to remote code execution, enabling threat actors to gain unauthorized access and control over affected systems. The vulnerability is actively being exploited in the wild.

Vulnerability Details:

- **Vulnerability ID**: CVE-2023-39469
- **CVSS Score**: 7.2 (High)
- **Severity**: High
- **Type:** Remote Code Execution via insecure scripting configuration
- **CWE Reference**: CWE-94 (Improper Control of Generation of Code)
- **Affected Versions**: PaperCut NG/MF: Versions prior to 22.1.1
- **Fixed Versions**: PaperCut NG/MF v22.1.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating PaperCut to the latest, fixed version 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://www.papercut.com/kb/Main/SecurityBulletinJune2023