ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

NOTE DE SECURITE

Titre	Exploitation active d'une vulnérabilité critique dans PaperCut MF (Multifonction) et NG (Nouvelle Génération)
Numéro de Référence	41901505/23
Date de Publication	15 Mai 2023
Risque	Critique
Impact	Critique

Des rapports font état de l'exploitation active d'une vulnérabilité critique (CVE-2023-27350) dans PaperCut MF (Multifunction) et NG (Next Generation). PaperCut MF et NG sont des solutions de gestion d'impression utilisées pour gérer et contrôler les activités d'impression et de copie dans les environnements d'impression en réseau des utilisateurs.

L'exploitation réussie de cette vulnérabilité pourrait permettre à un acteur non authentifié de réaliser une exécution de code à distance (RCE) sur les serveurs d'application PaperCut. Cette vulnérabilité serait également exploitée pour déployer des ransomwares sur le réseau des utilisateurs.

Un correctif de sécurité a été publié pour corriger cette faille critique. Veuillez se référer au bulletin de sécurité maCERT « 41710505 /23 » pour plus d'information.

La détection des tentatives d'exploitation doivent se concentrer sur les trois domaines clés suivants :

- Signatures du trafic réseau - Recherchez un trafic réseau anormal tentant d'accéder à la page "SetupCompleted" d'un serveur PaperCut exposé et vulnérable.
- Surveillance du système - Recherchez les sous processus créés à partir du processus "pc-app.exe" d'un serveur PaperCut.
- Paramètres du serveur et fichiers journaux - Recherchez des preuves d'activités malveillantes dans les paramètres du serveur PaperCut et dans les fichiers journaux.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Annexe

- https://www.papercut.com/kb/Main/PO-1216-and-PO-1219
- https://www.dgssi.gov.ma/fr/content/41710505-23-vulnerabilite-critique-dans-les-produits-papercut.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 57 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma