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

BULLETIN DE SECURITE

Titre	Vulnérabilité critique dans Microsoft Authenticator (Patch Tuesday Mars 2026)
Numéro de Référence	61881103/26
Date de Publication	11 Mars 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft Authenticator pour Android ;
- Microsoft Authenticator pour iOS ;

Identificateurs externes

- CVE-2026-26123 ;

Bilan de la vulnérabilité

Une vulnérabilité a été identifiée dans l'application Microsoft Authenticator. Cette faille pourrait permettre à une application malveillante de se faire passer pour Microsoft Authenticator et d'intercepter les informations d'authentification de l'utilisateur.

L'exploitation peut être déclenchée lorsque l'utilisateur sélectionne une application malveillante pour traiter le flux d'authentification, notamment via un lien malveillant ou un code QR frauduleux. Un attaquant pourrait obtenir suffisamment d'informations pour usurper l'identité de l'utilisateur et accéder à des services protégés par l'authentification multifacteur (MFA).

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 10 Mars 2026**.**

Risque

- Usurpation d'identité ;
- Contournement du mécanisme d'authentification multifacteur (MFA) ;
- Accès aux informations confidentielles.

Annexe

Bulletin de sécurité Microsoft du 10 Mars 2026**:**

- https://msrc.microsoft.com/update-guide/

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