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	Vulnérabilités critiques dans plusieurs produits Microsoft (Patch Tuesday Février 2025)
Numéro de Référence	52601202/25
Date de Publication	12 Février 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- CBL Mariner 2.0 ARM
- CBL Mariner 2.0 x64
- Microsoft Outlook pour Android
- Microsoft PC Manager
- Microsoft Surface Go 2
- Microsoft Surface Go 3
- Microsoft Surface Hub
- Microsoft Surface Hub 2S
- Microsoft Surface Hub 3
- Microsoft Surface Laptop Go
- Microsoft Surface Laptop Go 2
- Microsoft Surface Laptop Go 3
- Microsoft Surface Pro 7+
- Microsoft Surface Pro 8
- Microsoft Surface Pro 9 ARM
- Surface Laptop 3 with Intel Processor
- Surface Laptop 4 with AMD Processor
- Surface Laptop 4 with Intel Processor
- Surface Windows Dev Kit

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

Identificateurs externes

- CVE-2025-21371 CVE-2025-21200 CVE-2025-21418
- CVE-2025-21368 CVE-2025-21373 CVE-2025-21322
- CVE-2025-21181 CVE-2025-21377 CVE-2025-21359
- CVE-2025-21350 CVE-2025-21347 CVE-2025-21337
- CVE-2025-21201 CVE-2025-21190 CVE-2025-21410
- CVE-2025-21407 CVE-2025-21406 CVE-2025-21208
- CVE-2025-21194 CVE-2025-21259 CVE-2023-32002
- CVE-2025-21420 CVE-2025-21419 CVE-2025-21376
- CVE-2025-21375 CVE-2025-21369 CVE-2025-21352

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques affectant les produits Microsoft susmentionnés. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant d'exécuter du code arbitraire à distance, de réussir une élévation de privilèges, de causer un déni de service, une usurpation d'identité et de de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 11 Février 2025**.**

Risque

- Exécution du code arbitraire à distance
- Contournement de la politique de sécurité
- Elévation de privilèges
- Usurpation d'identité
- Déni de service

Annexe

Bulletin de sécurité Microsoft du 11 Février 2025**:**

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