



BULLETIN DE SECURITE

Titre	Vulnérabilités dans plusieurs produits Microsoft (Patch Tuesday Octobre 2024)
Numéro de Référence	50060910/24
Date de Publication	09 Octobre 2024
Risque	Important
Impact	Important

Systemes affectés

- CBL Mariner 2.0 ARM
- CBL Mariner 2.0 x64
- Microsoft Configuration Manager 2303
- Microsoft Configuration Manager 2309
- Microsoft Configuration Manager 2403
- Microsoft Defender pour Endpoint pour Linux
- Microsoft Outlook pour Android

Identificateurs externes

- CVE-2024-43611 CVE-2024-43593 CVE-2024-43547 CVE-2024-43468
- CVE-2024-38262 CVE-2024-43614 CVE-2024-43583 CVE-2024-43599
- CVE-2024-43592 CVE-2024-43589 CVE-2024-43572 CVE-2024-43570
- CVE-2024-43567 CVE-2024-43564 CVE-2024-43563 CVE-2024-43560
- CVE-2024-43556 CVE-2024-43553 CVE-2024-43550 CVE-2024-43549
- CVE-2024-43545 CVE-2024-43544 CVE-2024-43521 CVE-2024-43520
- CVE-2024-43517 CVE-2024-43514 CVE-2024-43512 CVE-2024-43509
- CVE-2024-43501 CVE-2024-43456 CVE-2024-38212 CVE-2024-43453
- CVE-2024-38265 CVE-2024-38124 CVE-2024-38149 CVE-2024-37983
- CVE-2024-37979 CVE-2024-37982 CVE-2024-37976 CVE-2024-43607
- CVE-2024-43608 CVE-2024-43604 CVE-2024-6197 CVE-2024-43573

- CVE-2024-43541 CVE-2024-43535 CVE-2024-43534 CVE-2024-43532
- CVE-2024-43519 CVE-2024-43518 CVE-2024-43515 CVE-2024-43513
- CVE-2024-43506 CVE-2024-38261

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant les produits Microsoft susmentionnés. L'exploitation de ces failles peut permettre à un attaquant d'exécuter du code arbitraire, porter atteinte à la confidentialité des données, de causer un déni de service et de contourner la politique de sécurité.

Solution

Veillez se référer au bulletin de sécurité Microsoft du 08 Octobre 2024.

Risque

- Déni de service
- Exécution de code à distance
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité Microsoft du 08 Octobre 2024:

- <https://msrc.microsoft.com/update-guide/fr-FR>