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 Microsoft Windows (Patch Tuesday Juin 2025)
Numéro de Référence	55021106 /25
Date de Publication	11 Juin 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 pour x64-based Systems
- Windows 10 Version 1607 pour 32-bit Systems
- Windows 11 Version 23H2 pour x64-based Systems
- Windows 11 Version 23H2 pour ARM64-based Systems
- Windows Server 2025 (Server Core installation)
- Windows 10 Version 22H2 pour 32-bit Systems
- Windows 10 Version 22H2 pour ARM64-based Systems
- Windows 10 Version 22H2 pour x64-based Systems
- Windows 11 Version 22H2 pour x64-based Systems
- Windows 11 Version 22H2 pour ARM64-based Systems
- Windows 10 Version 21H2 pour x64-based Systems
- Windows 10 Version 21H2 pour ARM64-based Systems
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows 10 Version 21H2 pour 32-bit Systems
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019

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

- Windows 10 Version 1809 pour x64-based Systems
- Windows 10 Version 1809 pour 32-bit Systems
- Windows 10 pour x64-based Systems
- Windows 10 pour 32-bit Systems
- Windows Server 2025
- Windows 11 Version 24H2 pour x64-based Systems
- Windows 11 Version 24H2 pour ARM64-based Systems
- Windows Security App
- Remote Desktop client pour Windows Desktop
- Windows App Client pour Windows Desktop

Identificateurs externes

- CVE-2025-33073 CVE-2025-33057 CVE-2025-33053
- CVE-2025-47955 CVE-2025-33075 CVE-2025-33065
- CVE-2025-33061 CVE-2025-32724 CVE-2025-32720
- CVE-2025-32716 CVE-2025-32713 CVE-2025-3052
- CVE-2025-33070 CVE-2025-33069 CVE-2025-33068
- CVE-2025-33056 CVE-2025-33055 CVE-2025-33052
- CVE-2025-33050 CVE-2025-32725 CVE-2025-24065
- CVE-2025-24069 CVE-2025-24068 CVE-2025-47969
- CVE-2025-33071 CVE-2025-47956 CVE-2025-47160
- CVE-2025-33067 CVE-2025-33066 CVE-2025-33064
- CVE-2025-33063 CVE-2025-33062 CVE-2025-33060
- CVE-2025-33059 CVE-2025-33058 CVE-2025-32722
- CVE-2025-32721 CVE-2025-32719 CVE-2025-32718
- CVE-2025-32715 CVE-2025-32714 CVE-2025-32712
- CVE-2025-32710 CVE-2025-29828

Bilan de la vulnérabilité

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

Microsoft confirme que le zero-day «CVE-2025-33053» est activement exploitée permettant à un attaquant l'exécution du code arbitraire à distance via l'envoi des liens malicieux.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 10 Juin 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 10 Juin 2025**:**

- 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