ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant Microsoft Windows ESU (Patch Tuesday Mars 2025)
Numéro de Référence	53181203/25
Date de Publication	12 Mars 2025
Risque	Important
Impact	Critique

Systèmes affectés

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)
- Windows Server 2012
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1

Identificateurs externes

CVE-2024-9157 CVE-2025-21180 CVE-2025-21247 CVE-2025-24035 CVE-2025-24044
CVE-2025-24045 CVE-2025-24051 CVE-2025-24054 CVE-2025-24055 CVE-2025-24056
CVE-2025-24059 CVE-2025-24064 CVE-2025-24071 CVE-2025-24072 CVE-2025-24983
CVE-2025-24984 CVE-2025-24985 CVE-2025-24987 CVE-2025-24988 CVE-2025-24991
CVE-2025-24992 CVE-2025-24993 CVE-2025-24996 CVE-2025-26633 CVE-2025-26645

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant les versions susmentionnées de son système d'exploitation Windows. Plusieurs de ces vulnérabilités sont des Zero-days susceptibles d'être activement exploités. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'élévation de privilèges, l'exécution de code arbitraire, l'accès à des données confidentielles ou le contournement de mesures de sécurité.

Solution

Veuillez se référer aux bulletins de sécurité de Microsoft pour obtenir les nouvelles mises à jour

Risque

- Elévation de privilèges
- Exécution de code arbitraire
- Accès à des données confidentielles
- Contournement de mesures de sécurité

Référence

Guide de sécurité de Microsoft :

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

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma