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 Décembre 2024)
Numéro de Référence	51431112/24
Date de Publication	11 Décembre 2024
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-2024-49112	CVE-2024-49085	CVE-2024-49086	CVE-2024-49102
CVE-2024-49104	CVE-2024-49125	CVE-2024-49080	CVE-2024-49120
CVE-2024-49128	CVE-2024-49126	CVE-2024-49127	CVE-2024-49122
CVE-2024-49118	CVE-2024-49124	CVE-2024-49072	CVE-2024-49138
CVE-2024-49088	CVE-2024-49090	CVE-2024-49079	CVE-2024-49129
CVE-2024-49121	CVE-2024-49113	CVE-2024-49096	CVE-2024-49089
CVE-2024-49091	CVE-2024-49084	CVE-2024-49082	

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. Une de ces vulnérabilités, identifiée par « CVE-2024-49138 » est un Zero-Day activement exploité. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'élévation de privilèges, l'exécution de code arbitraire ou l'accès à des données confidentielles

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

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