AVIS DE SECURITE

Objet	**Multiples vulnérabilités critiques dans les produits Microsoft**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-260
TLP	WHITE

Résumé

Microsoft a publié le 13/10/2026 son Patch Tuesday d'octobre 2026, qui corrige plusieurs centaines de vulnérabilités dans Windows (client et serveur), Exchange Server, SQL Server, .NET, SharePoint Server et d'autres composants. Cinq vulnérabilités (CVE-2026-96951, CVE-2026-56155, CVE-2026-85880, CVE-2026-81963, CVE-2026-32202) sont activement exploitées selon le catalogue CISA KEV. Plusieurs failles de type exécution de code à distance, avec un score CVSS v3 de 9.8, touchent notamment RDP, DHCP Server, MSMQ, le service FTP et les pilotes réseau ; la plus sévère (CVE-2026-57092, Windows VMSwitch) atteint un CVSS de 9.9.

Risque de sécurité

- Exécution de code arbitraire à distance
- Élévation de privilèges
- Contournement de la politique de sécurité
- Usurpation d'identité (spoofing)
- Atteinte à la confidentialité des données

Systèmes affectés

- Windows 10 (1607, 1809, 21H2) et Windows 11 (23H2 à 26H1)
- Windows Server 2012 à 2025 (dont RDP, DHCP Server, MSMQ, service FTP, VMSwitch/Hyper-V, ALPC, Windows Update Stack)
- Microsoft Exchange Server 2016 (CU23), 2019 (CU14 et CU15) et Subscription Edition (CVSS jusqu'à 9.3)
- Microsoft SQL Server 2017, 2019, 2022 et 2025, et pilote ODBC (CVE-2026-42990, CVSS 9.8)
- Microsoft .NET Framework, .NET 8, 9 et 10 (CVSS jusqu'à 9.4)
- SharePoint Server Subscription Edition, Office Online Server et Skype for Business Server (CVSS 8.8)
- Active Directory Federation Services (CVE-2026-56155, exploitée)

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 13/10/2026 :

- https://msrc.microsoft.com/update-guide/releaseNote/2026-Oct (notes de version Microsoft d'octobre 2026)
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog (vulnérabilités exploitées : CVE-2026-96951, 56155, 85880, 81963, 32202)

2. Appliquer en priorité les mises à jour de sécurité Microsoft d'octobre 2026 sur les systèmes exposés (RDP, DHCP, Exchange, hyperviseurs Hyper-V) et sur les postes affectés par les failles exploitées.
3. Mettre à jour Exchange Server (KB5128895 à KB5128898 et KB5129955 à KB5129958) et SQL Server (KB5126934, KB5126967, KB5128492 à KB5128497).

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar https://www.stcc-ssi.sn/	E-mail : sncsirt@dcssi.sn	Date de publication : 14/10/2026