AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SÉCURITÉ

Microsoft Outlook : vulnérabilité zero day activement exploitée

Contenu

I. Contexte 3
II. Vulnérabilité identifiée 3
Versions affectées et corrigées 4
III. Vecteur d'attaque 4
IV. Menaces actives 4
V. Exposition de l'Afrique et du Cameroun 5
VI. Conclusion et actions recommandées 5
VII. Références 5

I. Contexte

Le 10 novembre 2026, à l'occasion de son Patch Tuesday mensuel, Microsoft a corrigé 1 094 vulnérabilités dans ses produits. Parmi elles figure une faille de Microsoft Outlook, référencée CVE-2026-124194, que l'éditeur confirme comme activement exploitée par des attaquants. Il s'agit de la seule vulnérabilité zero day exploitée de cette publication.

Le même jour, l'agence américaine CISA a ajouté cette faille à son catalogue des vulnérabilités connues pour être exploitées (KEV) et a fixé au 24 novembre 2026 la date limite de correction pour les agences fédérales américaines. Bien que son score CVSS soit modéré, son exploitation active en fait une priorité absolue.

II. Vulnérabilité identifiée

La faille est une vulnérabilité d'usurpation (spoofing) liée au fait que l'interface d'Outlook n'avertit pas l'utilisateur lors d'actions dangereuses (CWE 356). Elle permet à un attaquant non autorisé de mener une attaque d'usurpation à travers le réseau et, en pratique, de dérober le condensat d'authentification NTLMv2 de l'utilisateur.

CVE	CVE-2026-124194
Produit	Microsoft Outlook pour Windows
Type	Usurpation (spoofing), absence d'avertissement sur action dangereuse (CWE 356)
Impact	Fuite du condensat NTLMv2 et usurpation de l'identité de l'utilisateur
Score CVSS v3	**6.5 (Modéré)**
Statut	**Activement exploitée, inscrite au catalogue KEV de la CISA**
Interaction utilisateur	Ouverture d'un fichier de message piégé
Date de publication	10 novembre 2026
Correctif	Mises à jour de sécurité Office de novembre 2026

Versions affectées et corrigées

Les versions suivantes d'Outlook pour Windows sont affectées. Pour Microsoft 365 Apps, le numéro de build corrigé dépend du canal de mise à jour utilisé et figure dans les notes de publication de sécurité Office du 10 novembre 2026.

Produit	Versions affectées	Versions corrigées
Microsoft 365 Apps for Enterprise	Builds antérieurs aux mises à jour de novembre 2026	Build de novembre 2026 selon le canal
Office LTSC 2021	Antérieures au build 16.0.14334.21048	16.0.14334.21048 ou ultérieur
Office LTSC 2024	Antérieures au build 16.0.17932.21140	16.0.17932.21140 ou ultérieur

III. Vecteur d'attaque

L'exploitation observée se déroule comme suit :

- L'attaquant envoie à la victime un fichier de message spécialement conçu, généralement par courriel.
- La victime est incitée par ingénierie sociale à ouvrir ce fichier dans Outlook.
- Outlook se connecte alors à une ressource réseau contrôlée par l'attaquant, sans afficher l'avertissement habituel relatif au contenu externe.
- Lors de cette connexion, Outlook transmet le condensat NTLMv2 de l'utilisateur, que l'attaquant peut réutiliser pour s'authentifier sous son identité ou tenter de retrouver son mot de passe.

Selon Microsoft, le volet de lecture (Preview Pane) ne constitue pas un vecteur d'attaque : l'ouverture du fichier par l'utilisateur reste nécessaire.

IV. Menaces actives

Microsoft et la CISA confirment l'exploitation active de cette vulnérabilité. L'éditeur n'a pas encore communiqué l'identité des attaquants, le nombre de victimes ni d'indicateurs de compromission. Selon les informations disponibles, un code d'exploitation fonctionnel existerait déjà.

Le vol de condensats NTLM est une technique largement utilisée par les groupes de rançongiciels et les acteurs étatiques pour s'introduire dans les réseaux d'entreprise, se déplacer latéralement et élever leurs privilèges, en particulier dans les environnements Active Directory.

V. Exposition de l'Afrique et du Cameroun

Microsoft Outlook est le client de messagerie le plus utilisé au sein des administrations publiques, des banques, des opérateurs de télécommunications et des entreprises camerounaises, très souvent couplé à un annuaire Active Directory.

Un seul utilisateur qui ouvre un fichier piégé peut fournir à un attaquant les éléments nécessaires pour accéder au réseau interne de toute une structure. Les postes dont les mises à jour Office sont différées ou non gérées de façon centralisée sont particulièrement exposés.

VI. Conclusion et actions recommandées

Cette vulnérabilité d'Outlook, déjà exploitée, permet de dérober les identifiants des utilisateurs par la simple ouverture d'un fichier piégé. Le CIRT recommande vivement les actions suivantes :

1. Installer sans délai les mises à jour de sécurité Office de novembre 2026 sur tous les postes disposant d'Outlook.
2. Pour Microsoft 365 Apps, vérifier que le canal de mise à jour utilisé a bien reçu le correctif et contrôler le numéro de build après installation.
3. Bloquer le trafic SMB sortant (port TCP 445) et l'authentification NTLM vers Internet au niveau du pare feu périmétrique.
4. Lorsque cela est possible, ajouter les comptes sensibles au groupe Protected Users et restreindre l'usage de NTLM au profit de Kerberos.
5. Surveiller les connexions SMB ou WebDAV sortantes inhabituelles initiées par le processus Outlook ainsi que les authentifications anormales.
6. Sensibiliser les utilisateurs à ne pas ouvrir de fichiers de message ou de pièces jointes inattendus, même provenant d'expéditeurs apparemment connus.
7. Appliquer également les autres correctifs du Patch Tuesday de novembre 2026, en priorité sur les contrôleurs de domaine et les serveurs exposés.

Pour tout incident ou toute demande d'assistance, contactez le CIRT via ses canaux habituels.

VII. Références

- Microsoft Security Update Guide, CVE-2026-124194 : msrc.microsoft.com
- CISA, catalogue Known Exploited Vulnerabilities : www.cisa.gov
- SecurityOnline, Outlook zero day CVE-2026-124194 : securityonline.info
- SecurityWeek, Patch Tuesday de novembre 2026 : www.securityweek.com