BULLETIN DE SECURITE NUMERIQUE

1. Informations générales	
Référence	**CERTBFA-2025-MEN-014**
Intitulé	Abus du mécanisme de sélection de fichiers OneDrive pour contourner les contrôles d'accès
Type	☐ Vulnérabilité ☐ Indicateurs de compromission ☒ Menace
Date	29/05/2025
Concernés	☒ Tous ☐ Autre : _____

2. Risques

- Accès non autorisé à tous les fichiers OneDrive (documents confidentiels, informations personnelles, données d'entreprise)
- Extraction de propriété intellectuelle et documents stratégiques
- Utilisation des données pour des attaques ciblées ultérieures
- Monitoring non détecté des activités et communications

3. Systèmes affectés

- Microsoft OneDrive File Picker (toutes versions)
- ChatGPT, Slack, Trello, ClickUp, et des centaines d'autres services web intégrés

4. Synthèse

Une vulnérabilité critique dans Microsoft OneDrive File Picker permet aux applications web tierces d'accéder à l'intégralité du stockage cloud des utilisateurs au lieu des seuls fichiers sélectionnés. Cette faille résulte d'une implémentation défaillante des scopes OAuth qui attribue des permissions excessivement larges et d'interfaces de consentement trompeuses.

5. Solutions/Recommandations/Correctifs

Pour les utilisateurs :

- Vérifier et révoquer les autorisations d'applications tierces inutiles dans les paramètres de confidentialité du compte Microsoft

Pour les organisations :

- Mettre en place des politiques de consentement administrateur
- Configurer des contrôles d'accès conditionnel bloquant les applications demandant plus que les permissions Files.Read

Pour les développeurs :

- Éviter les demandes d'accès hors ligne générant des jetons de rafraîchissement
- Implémenter un stockage sécurisé des jetons d'authentification

Pour les équipes sécurité :

- Surveiller les logs de l'API Graph et des solutions CASB pour détecter les accès anormaux à OneDrive

6. Références

https://cybersecuritynews.com/onedrive-file-picker-vulnerability/