AlerteCyber - Faille de sécurité critique dans Microsoft Outlook

Publié le 26 février 2024

Dans le cadre de la procédure « AlerteCyber », le Mouvement des entreprises de France vous transmet l'alerte que l'ANSSI et Cybermalveillance.gouv.fr nous ont fait parvenir ce jour.

Elle concerne une vulnérabilité critique et qui pourrait être massivement exploitée dans Microsoft Outlook, immatriculée CVE-2024-21413 alias MonikerLink. Les risques de vol, modification, voire destruction de données sont élevés. L'application des mises à jour de sécurité est à réaliser sans délai par les utilisateurs des versions concernées de cette application très fortement employée dans la sphère professionnelle.

Description

Une faille de sécurité critique a été corrigée dans le produit Microsoft Outlook de la suite Office pour Windows.

L'exploitation de cette vulnérabilité par une personne malveillante peut lui permettre la prise de contrôle à distance des équipements concernés et le vol, voire la destruction, d'informations confidentielles.

Des cybercriminels pourraient très prochainement exploiter cette vulnérabilité pour conduire des attaques massives contre les systèmes vulnérables.

Microsoft a publié une mise à jour qui corrige cette vulnérabilité et protège de son exploitation.

Systèmes concernés

- Microsoft Office 2016
- Microsoft Office 2019
- Microsoft Office LTSC 2021
- Microsoft 365 Apps

Mesures à prendre

Mettre à jour au plus vite les équipements concernés avec le correctif de sécurité mis à disposition par l'éditeur.

Procédure

Se référer au bulletin de sécurité de l'éditeur pour obtenir le correctif : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413

Besoin d'assistance ?

Vous pouvez trouver sur Cybermalveillance.gouv.fr des prestataires de proximité susceptibles de vous apporter leur soutien dans la mise en œuvre de ces mesures.