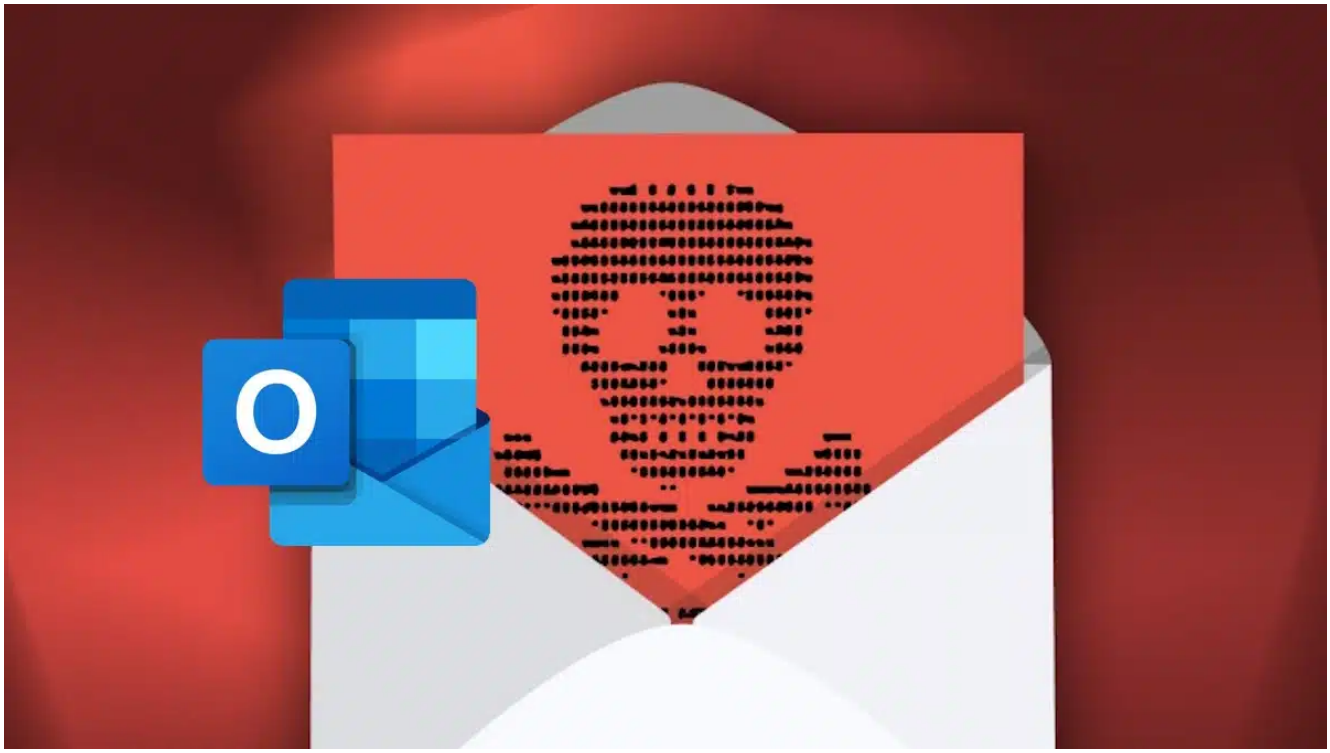
Faille critique dans Outlook et un simple courriel permet le contrôle à distance de votre ordinateur

Aymeric Geoffre-Rouland ⁝

Outlook, le client de messagerie de Microsoft, présente une vulnérabilité critique qui peut être exploitée par un e-mail contenant un lien malveillant.
Cette faille permet à un attaquant d'accéder aux fichiers de l'ordinateur de la victime.
Voici comment vous protéger de cette menace.



Attention à cette faille de sécurité Outlook © Tom's Guide

Outlook, le célèbre client de messagerie de Microsoft, présente **une vulnérabilité critique** qui peut être exploitée par des pirates informatiques.
Cette faille, nommée **CVE-2024-21413**, permet à un attaquant d'accéder aux fichiers de l'ordinateur de la victime en lui envoyant un courriel contenant un lien malveillant.
Voici comment vous protéger de cette menace.

Outlook : qu'est-ce que la faille CVE-2024-21413 ?

La faille CVE-2024-21413 est une vulnérabilité qui affecte Outlook.
Elle a été découverte par Haifei Li, un chercheur en sécurité chez Check Point.
Elle permet à un attaquant de bénéficier de **privilèges élevés sur l'ordinateur de la victime**, et ainsi de lire, écrire ou supprimer des fichiers.

Pour exploiter cette faille, l'attaquant doit envoyer un courriel à la victime, contenant un lien qui utilise le protocole file://.
Ce protocole permet d'accéder à des ressources distantes, comme des fichiers partagés sur un réseau.
Le lien doit indiquer le chemin vers le fichier à charger suivi d'un point d'exclamation et d'une chaîne aléatoire de caractères.
Si la victime clique sur le lien, Outlook ouvre le fichier en mode lecture seule, mais **l'attaquant peut alors exécuter du code malveillant** sur l'ordinateur de la victime.

La faille CVE-2024-21413 touche les versions suivantes de Microsoft Office :

- Microsoft 365 Apps for Enterprise,
- Microsoft Office 2021,
- Microsoft Office 2019,
- Microsoft Office 2016.

Cette faille est considérée comme critique, car elle peut être utilisée lors de campagnes de phishing, qui visent à tromper les utilisateurs en leur faisant croire qu'ils reçoivent un courriel légitime.
L'attaquant peut ainsi se faire passer pour **un contact de confiance**, un **service officiel** ou une **entreprise connue**.

À lire : Outlook : l'intelligence artificielle rédigera bientôt les e-mails à votre place

Pour se protéger de cette faille, il faut **mettre à jour sa version d'Office** avec le correctif de sécurité adéquat.
Le correctif a été diffusé lors du Patch Tuesday de février 2024, qui est le cycle mensuel de mises à jour de Microsoft.
Pour vérifier sa version d'Office et rechercher les mises à jour, il faut ouvrir Outlook > cliquer sur Fichier > Compte > Options de mise à jour.

Voici les versions d'Office qui contiennent le correctif :

- Office 2021 : Version 2401,
- Office LTSC 2021 : Version 2108,
- Office 2019 : Version 2401,
- Office 2019 : Version 1808,
- Office 2016 : Version 2401.

Pour les utilisateurs de Microsoft 365 Apps, le correctif dépend du canal de mise à jour choisi.
Voici les versions selon les différents canaux :

- Current Channel : Version 2401,
- Monthly Enterprise Channel : Version 2312,
- Monthly Enterprise Channel : Version 2311,
- Semi-Annual Enterprise Channel : Version 2308,
- Semi-Annual Enterprise Channel : Version 2302,
- Semi-Annual Enterprise Channel : Version 2208.

Source : Microsoft

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240215
"C'est ensemble qu'on avance"