Veille Technologique Passive : Cybersécurité en entreprise

Dans cette veille technologique, nous allons parler d’une faille de sécurité "zéro-click" corrigée dans Microsoft Outlook (CVE-2024-30103).

Nature de la Faille : Exécution de code à distance via un e-mail malveillant sans interaction de l'utilisateur. En effet, il suffit que l'e-mail soit ouvert ou prévisualisé dans Outlook pour que la vulnérabilité soit exploitée et que le code malveillant soit exécuté.

Impact : Affecte Outlook 2016 (32 et 64 bits), Office 2019 (32 et 64 bits), Office LTSC 2021 (32 et 64 bits) et Microsoft 365 Apps for Enterprise (32 et 64 bits)

Gravité : Notée 8.8 sur 10, sur l'échelle CVSS.

Correctif : Publié par Microsoft en juin 2024.

Recommandation : Mettre à jour Outlook dès que possible pour se protéger contre cette vulnérabilité critique.

Microsoft a publié des correctifs de sécurité le 11 juin, à l'occasion de la sortie de son Patch Tuesday de juin 2024, qui comprend notamment la correction de la faille de sécurité CVE-2024-30103.
Si on utilise Outlook 2016, il faut installer la KB5002600.
Pour les autres versions, il faut se référer au numéro de build de Microsoft Office qui correspond à la version publiée le 11 juin dernier.

Sources (Inoreader) :

- https://www.cve.org/CVERecord?id=CVE-2024-30103
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103
- https://www.it-connect.fr/microsoft-outlook-faille-de-securite-zero-click-cve-2024-30103/
- https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0485/