Veille Technologique Passive : Cybersécurité en entreprise

Dans cette veille technologique, nous allons parler du Patch Tuesday d'avril 2024, de Windows, avec la correction de 150 vulnérabilités et 2 failles zero-day (**CVE-2024-26234** et **CVE-2024-29988**).

- **CVE-2024-26234**, vulnérabilité dans le **pilote de Proxy** de Windows (spoofing). cette vulnérabilité est associée à un pilote malveillant signé avec un certificat "*Microsoft Hardware Publisher*" valide, ce qui lui permet d'être approuvé par le système d'exploitation Windows.
  Cette faille affecte **toutes les versions** de **Windows** et **Windows Server.**

- **CVE-2024-29988**, vulnérabilité dans la fonction **SmartScreen** de Windows (bypass). Microsoft a déjà publié plusieurs correctifs pour corriger cette faille, mais le patch parvient à être contourné. Ainsi, la faille de sécurité **CVE-2024-29988** permet de contourner le correctif **CVE-2024-21412**, qui lui-même permettait de contourner le correctif **CVE-2023-36025.**
  Cette faille affecte les versions, **Windows 10 Version 1809** et **versions supérieures** et **Windows Server 2019** et **versions supérieures**.

Pour régler ces failles, il suffit de **mettre à jour** votre système d'exploitation **Windows** et **Windows Server**. Grâce à Windows Update ou WSUS, pour les organisations. Et bien entendu de rester à l'affut, des éventuels bugs de ces mises à jour et se tenir au courant des nouvelles mises à joue à venir.

Sources (Inoreader) :

- https://www.it-connect.fr/microsoft-patch-tuesday-avril-2024-150-vulnerabilites-2-failles-zero-day/
- https://www.it-connect.fr/windows-patch-deux-failles-zero-day-exploitees-dans-attaques-malwares-avril-2024/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988