



BULLETIN DE SECURITE

Titre	Vulnérabilités dans plusieurs produits Microsoft (Patch Tuesday Janvier 2023)
Numéro de Référence	39731201/23
Date de Publication	12 Janvier 2023
Risque	Important
Impact	Important

Systemes affectés

- Microsoft 365 Apps pour Enterprise pour 64 bits Systems
- Microsoft 365 Apps pour Enterprise pour systèmes 32 bits
- Microsoft Visio 2013 Service Pack 1 (éditions 32 bits)
- Microsoft Visio 2013 Service Pack 1 (éditions 64 bits)
- Microsoft Visio 2016 (édition 32 bits)
- Microsoft Visio 2016 (édition 64 bits)
- Visual Studio Code
- 3D Builder

Identificateurs externes

- CVE-2023-21741 , CVE-2023-21734 , CVE-2023-21762 , CVE-2023-21761 , CVE-2023-21792 , CVE-2023-21790 , CVE-2023-21789 , CVE-2023-21779 , CVE-2023-21745 , CVE-2023-21764 , CVE-2023-21763 , CVE-2023-21738 , CVE-2023-21737 , CVE-2023-21788 , CVE-2023-21787 , CVE-2023-21785 , CVE-2023-21783 , CVE-2023-21793 , CVE-2023-21791 , CVE-2023-21786 , CVE-2023-21784 , CVE-2023-21782 , CVE-2023-21781 , CVE-2023-21780 , CVE-2023-21736 , CVE-2023-21735

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant les produits Microsoft susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant de réussir une élévation de privilèges, d'exécuter du code arbitraire à distance et de porter atteinte à la confidentialité de données.

Solution

Veillez se référer au bulletin de sécurité Microsoft du 10 janvier 2023.

Risque

- Elévation de privilèges
- Exécution du code arbitraire à distance
- Atteinte à la confidentialité de données

Annexe

Bulletin de sécurité Microsoft du 10 janvier 2023:

- <https://msrc.microsoft.com/update-guide/fr-FR>