Mouvement des Entreprises de France

AlerteCyber - Compromission de l'application 3CX Electron Desktop App

Publié le 13 avril 2023

Nous vous invitons à diffuser massivement cette alerte cyber pour se prémunir d'une faille de sécurité critique détectée dans cette application de conférence vocale et vidéo.

Risques

Espionnage, détournement de fonds, vol, voire destruction de vos données suite à la prise de contrôle à distance de vos ordinateurs concernés.

Description

Certaines versions de l'application de conférence vocale et vidéo 3CX Electron Desktop App ont été compromises par des cybercriminels en y intégrant un programme malveillant de type porte dérobée.

L'exploitation de ces versions infectées par un acteur malveillant peut lui permettre de se connecter à distance à tout ordinateur sur lequel l'application compromise a été installée pour réaliser diverses actions frauduleuses (espionnage, attaque par rançongiciel, vol de données, détournement de fonds...), voire de prendre le contrôle du réseau informatique de l'organisation concernée.

Systèmes concernés

3CX Electron Desktop App (application de bureau) :
3CX Electron Desktop App pour Windows versions 18.12.407 et 18.12.416
3CX Electron Desktop App pour macOS versions 18.11.1213, 18.12.402, 18.12.407 et 18.12.416

Mesures à prendre

Désinstaller les versions compromises de 3CX Electron Desktop App pour supprimer toute trace de la porte dérobée.

Vérifier si les postes sur lesquels l'application compromise était installée n'ont pas fait l'objet d'une attaque exploitée.

Bien que l'éditeur propose une nouvelle version corrigée de Electron Desktop App, 3CX recommande de privilégier l'utilisation de la version Web de son application (PWA).

Plus d'informations dans l'alerte ANSSI / CERT-FR citée en référence.

Procédure

Se référer au bulletin de sécurité de l'éditeur.

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.