aDvens

Security for the greater good

Newscast

Vulnérabilité critique 3CX

2023-03-31 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. CVE-2023-29059 - Compromission Supply Chain 3CX

3CX est une entreprise proposant des solutions de communication, intégrant une application de visioconférence. La société équiperait 600 000 clients dans 190 pays avec plus de 12 millions d'utilisateurs.

Le 29 mars 2023, l'application *3CXDesktopApp* a fait l'objet de signalements d'activités malveillantes par plusieurs solutions de sécurité, à la suite de la mise à jour *Update 7* du 22 mars. Cette dernière embarque un code malveillant permettant de déployer un implant de type infostealer pour dérober des informations des navigateurs des postes compromis.

Les premières communications vers les serveurs C2 se font 7 jours après la compromission. Les adresses des serveurs sont encodées dans un fichier *ICO*, récupéré sur un dépôt github.

Cette nouvelle attaque de type supply chain démontre une nouvelle fois que les fournisseurs restent un vecteur d'infection privilégié.

1.1. Produits impactés

- 3CXDesktopApp Electron pour Windows versions 18.12.407 et 18.12.416.
- 3CXDesktopApp Electron pour Mac versions 18.11.1213, 18.12.402, 18.12.407 et 18.12.416.

1.2. Recommandations

En l'absence de correctif, il est recommandé de désinstaller l'application *desktop* et de privilégier le *client web*.

Des informations complémentaires sont disponibles dans l'alerte de 3CX.

1.3. IoCs

TYPE	VALEUR
URL	github.com/IconStorages/images
Email	cliego.garcia@proton[.]me
Email	philip.je@proton[.]me
SHA-1	cad1120d91b812acafef7175f949dd1b09c6c21a
SHA-1	bf939c9c261d27ee7bb92325cc588624fca75429
SHA-1	20d554a80d759c50d6537dd7097fed84dd258b3e
URI	hxxps://www.3cx.com/blog/event-trainings/
URI	hxxps://akamaitechcloudservices.com/v2/storage
URI	hxxps://azureonlinestorage.com/azure/storage

TYPE	VALEUR
URI	hxxps://msedgepackageinfo.com/microsoft-edge
URI	hxxps://glcloudservice.com/v1/console
URI	hxxps://pbxsources.com/exchange
URI	hxxps://msstorageazure.com/window
URI	hxxps://officestoragebox.com/api/session
URI	hxxps://visualstudiofactory.com/workload
URI	hxxps://azuredeploystore.com/cloud/services
URI	hxxps://msstorageboxes.com/office
URI	hxxps://officeaddons.com/technologies
URI	hxxps://sourceslabs.com/downloads
URI	hxxps://zacharryblogs.com/feed
URI	hxxps://pbxcloudeservices.com/phonesystem
URI	hxxps://pbxphonenetwork.com/voip
URI	hxxps://msedgeupdate.net/Windows

2. Références

- https://www.3cx.com/blog/news/desktopapp-security-alert/
- https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/
- https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/
- https://news.sophos.com/en-us/2023/03/29/3cx-dll-sideloading-attack/
- https://nakedsecurity.sophos.com/2023/03/30/supply-chain-blunder-puts-3cx-telephone-app-users-at-risk/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29059