BOLETÍN DE ALERTA

Boletín Nro.: 2023-12
Fecha de publicación: 31/03/2023
Tema: Nuevo *malware* afecta al *software* 3CX DesktopApp

Software afectado:

- 3CX DesktopApp, versiones 18.12.407 y 18.12.416.

Descripción:

Se han reportado avisos recientes de incidentes sobre un nuevo *malware* que afecta al *software* empresarial 3CX DesktopApp. El mismo permitiría a los atacantes obtener información del sistema y secuestrar tanto los datos como las credenciales de inicio de sesión almacenadas de los perfiles de usuarios, en los navegadores web como Chrome, Edge, Brave y Firefox. Este afecta al cliente Windows Electron para clientes utilizando el Update 7.

La aplicación 3CX es un *software* de intercambio automático privado (*PABX*) que proporciona varias funciones de comunicación para sus usuarios, incluyendo videoconferencia, chat en vivo y gestión de llamadas. La aplicación está disponible en la mayoría de los principales sistemas operativos, incluidos Windows, macOS y Linux. Además, la versión de cliente está disponible en forma de aplicación móvil para dispositivos Android e iOS, mientras que una extensión de Chrome y la versión *PWA* del cliente permiten a los usuarios acceder al *software* a través de sus navegadores.

A fines de marzo de 2023, investigadores de seguridad revelaron que este popular *software* de comunicación empresarial fue víctima de atacantes. Los informes mencionan que se estaba utilizando una versión de cliente de escritorio 3CX VoIP (*Voice over Internet Protocol*) como parte de un ataque a los demás clientes 3CX.

Impacto:

La explotación exitosa de este *malware* permitiría a un atacante no autenticado obtener credenciales de acceso de los usuarios y acceder al sistema afectado.

Indicadores de compromiso (*IoC*):

SHA256	Nombre de archivo	Nombre de detección
dde033480755127962413 89dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc **Instalador:** aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868	3cxdesktopapp-18.12.407.msi (Windows)	Trojan.Win64.DEEFFACE.A
fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405 **Instalador:** 59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c098	3cxdesktopapp-18.12.416.msi (Windows)	Trojan.Win64.DEEFFACE.A
92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61 **Instalador:** 5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290	3CXDesktopApp-18.11.1213.dmg (macOS)	
b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb **Instalador:** e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec	3cxdesktopapp-latest .dmg (macOS)	
c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02	ffmpeg.dll	Trojan.Win64.DEEFFACE.A
7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896	ffmpeg.dll	Trojan.Win64.DEEFFACE.A
11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03	d3dcompiler.dll	Trojan.Win64.DEEFFACE.A
4e08e4ffc699e0a1de4a5225a0b4920933fbb9cf123cde33e1674fde6d61444f		

Prevención:

Las organizaciones potencialmente afectadas deben dejar de utilizar la versión vulnerable y aplicar los futuros parches o las soluciones de mitigación temporal. Los equipos de TI y seguridad también deben utilizar métodos de protección de binarios y monitorear los procesos de 3CX, con un enfoque particular en el tráfico *command-and-control (C&C).*

También, habilitar el monitoreo del comportamiento en productos de seguridad puede ayudar a detectar la presencia del ataque dentro del sistema.

Mitigación:

Si bien aún no se cuenta con un parche oficial que subsane el ataque de este *malware*, se recomienda desinstalar la aplicación de escritorio y utilizar el cliente *Progressive Web App* (*PWA*) de manera temporal hasta el lanzamiento de parches o nuevas versiones subsanadas. Es posible acceder al cliente *PWA* en la siguiente URL:

- https://www.3cx.com/blog/releases/web-client-pwa/
- https://www.3cx.es/blog/alerta-seguridad-desktop-app/

Información adicional:

- https://www.trendmicro.com/en_us/research/23/c/information-on-attacks-involving-3cx-desktop-app.html
- https://www.3cx.com/community/threads/3cx-desktopapp-security-alert.119951/
- https://www.3cx.com/blog/change-log/web-client-desktop-app/
- https://www.3cx.com/blog/releases/web-client-pwa/
- https://www.bleepingcomputer.com/news/security/hackers-compromise-3cx-desktop-app-in-a-supply-chain-attack/
- https://thehackernews.com/2023/03/3cx-desktop-app-targeted-in-supply.html