BOLETÍN DE ALERTA

Boletín Nro.: 2023-12
Fecha de publicación: 31/03/2023
Fecha de actualización: 03/04/2023
Tema: *Software cliente VoIP* de 3CX comprometido por ataque a la cadena de suministro - Actualización

Software afectado:

- 3CX DesktopApp (Windows), versiones 18.12.407 y 18.12.416.
- 3CX DesktopApp (macOS), versiones 18.11.1213, 18.12.402, 18.12.407 y 18.12.416.

Descripción:

Se han reportado nuevos avisos de incidentes sobre una campaña campaña de ataque a la cadena de suministro para la distribución de malware de tipo troyano, que sustituye a las versiones legítimas del *software* empresarial 3CX DesktopApp. El mismo permitiría a los atacantes a través de la versión modificada del *software* (*malware* troyano) 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.

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, que reemplazaron el auténtico por uno modificado maliciosamente. 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.

Actualmente, se ha reportado una vulnerabilidad vinculada al *malware,* identificada como CVE-2023-29059, sin severidad ni puntuación asignada aún. Esta vulnerabilidad de código malicioso embebido es consecuencia del ataque sufrido por el fabricante de 3CX DesktopApp. El troyano distribuido utiliza para esto varias *shellcode* ejecutadas desde el espacio de almacenamiento dinámico, desde el cual se carga una *DLL* a través de una explotación con nombre 'DllGetClassObject'. En esta etapa a su vez se descargan diferentes archivos de íconos desde un repositorio alojado en GitHub, que contiene información codificada en

BASE64 para una posterior descarga de otras funcionalidades. Esto permitiría a un atacante a través de la explotación de las versiones vulneradas instaladas en los dispositivos de la víctima, obtener información confidencial del sistema afectado.

Impacto:

La *presencia de la versión troyanizada de* DesktopApp 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		

Mitigación:

El fabricante recomienda utilizar la aplicación web (*PWA*) en sustitución de DesktopApp, es decir, se debe acceder a 3CX a través de un navegador, en lugar de con la aplicación de escritorio. Para los usuarios que cuenten con instalaciones "Self Hosted" y "On Premise", se recomienda instalar la actualización siguiendo los siguientes pasos:

- Iniciar la consola de gestión.
- Ir a la sección Actualizaciones.
- Descargar Mac Desktop App - 18.12.422.
- Descargar Windows Desktop App - 18.12.422.

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
- https://nvd.nist.gov/vuln/detail/CVE-2023-29059
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/campana-distribucion-software-troyanizado-3cx-desktopapp
- https://securityonline.info/cve-2023-29059-unraveling-the-trojanized-3cx-desktop-app-supply-chain-attack/