Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATAQUE A LA CADENA DE SUMINISTRO 3CX.

31/Marzo/2023

CONTENIDO

INTRODUCCIÓN.

El fabricante de software de comunicaciones empresariales 3CX confirmó el jueves que múltiples versiones de su aplicación de escritorio para Windows y macOS están afectadas por un ataque a la cadena de suministro.

Los números de versión incluyen 18.12.407 y 18.12.416 para Windows y 18.11.1213, 18.12.402, 18.12.407 y 18.12.416 para macOS. La compañía dijo que está contratando los servicios de Mandiant, propiedad de Google, para revisar el incidente. Mientras tanto, está instando a sus clientes de versiones locales y auto hospedadas del software a actualizar a la versión 18.12.422.

ATAQUE A LA CADENA DE SUMINISTROS ACX.

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_03_31_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	31/03/2023
Es día cero (0 day):	No

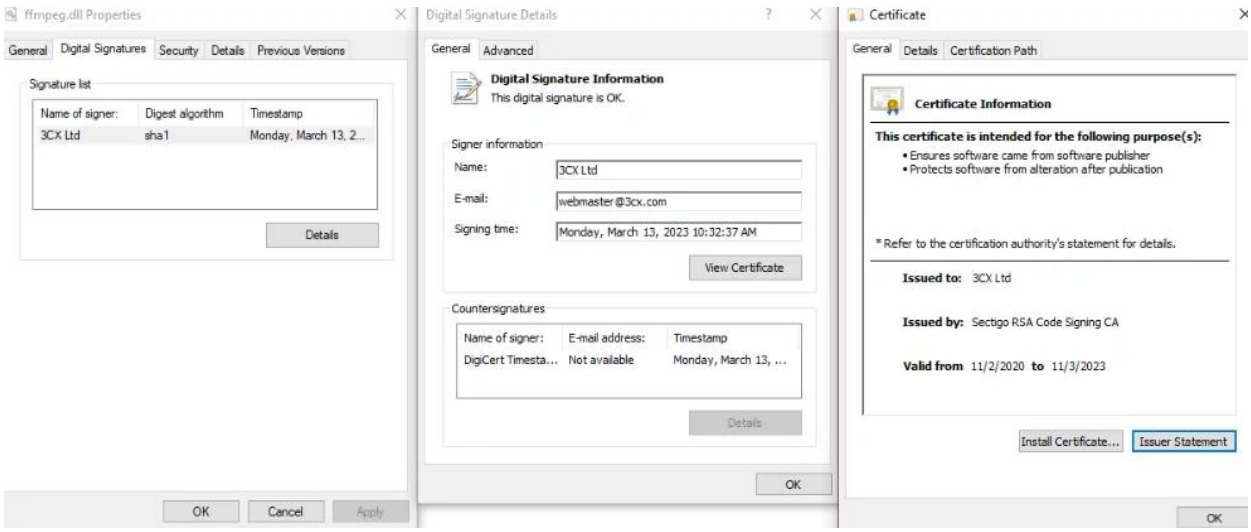
RESUMEN

El fabricante de software de comunicaciones empresariales 3CX confirmó el jueves que múltiples versiones de su aplicación de escritorio para Windows y macOS están afectadas por un ataque a la cadena de suministro.

ANÁLISIS TÉCNICO.

La evidencia disponible hasta el momento apunta a un compromiso de la canalización de compilación de software de 3CX para distribuir las versiones de Windows y macOS del paquete de la aplicación o, alternativamente, el envenenamiento de una dependencia ascendente. Las consecuencias completas de este incidente en la cadena de suministro aún están por verse.

La versión de Windows del ataque aprovechó una técnica llamada DLL side-loading para cargar una biblioteca no autorizada conocida como “ffmpeg.dll” que está diseñada para leer shellcode cifrado de otra DLL llamada “d3dcompiler_47.dll“, con una firma digital válida.

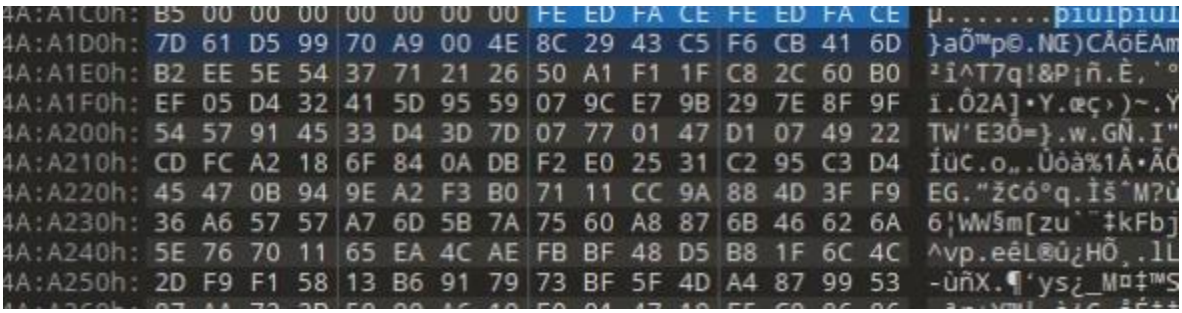


El descargador también es un archivo DLL con una función de exportación: DllGetClassObject : contiene todas las funciones maliciosas (DllEntryPoint no realiza ninguna actividad). En primer lugar, el descargador intenta abrir el archivo de manifiesto que contiene 4 bytes que representan el tiempo en segundos en que debe iniciarse la aplicación.

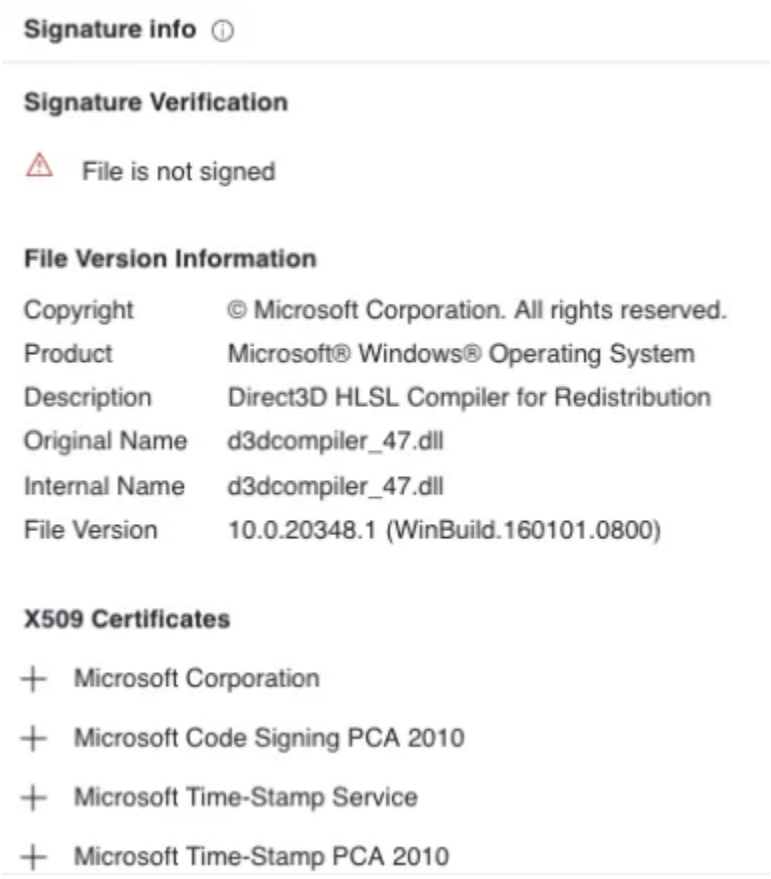
El DllEntryPoint conduce a la función maliciosa principal, que es responsable de leer el archivo d3dcompiler_47.dll que debe estar ubicado en el mismo directorio que el archivo ejecutable. Este archivo contiene un shellcode encriptado responsable de desempaquetar y ejecutar la siguiente etapa, que es un descargador. Es importante tener en cuenta que antes de extraer el shellcode, la DLL infectada crea un evento con el nombre AVMonitorRefreshEvent . El shellcode en sí se encuentra en la segunda DLL después de los bytes FEEDFACE :

```
index = 0i64;
while ( payload[index] != 0xFE
     || payload_[index - 2] != 0xED
     || payload_[index - 1] != 0xFA
     || payload_[index] != 0xCE )
{
  if ( v9 == ++index )
    goto LABEL_30;
}
```

El código que busca el inicio de la shellcode.



Vale la pena señalar que d3dcompiler_47.dll también tiene una firma digital, pero no es válida en este caso:



En comparación con la versión de Windows de la aplicación 3CX, su versión para Mac OS tiene una lógica ligeramente diferente. La aplicación contiene libffmpeg.dylib con dos sublibs dentro: para código arm64 y x86_64. El código malicioso se implementa en _run_avcodec(), que solo se puede encontrar en x86_64 sublib. La versión ARM64 no contiene el código malicioso. Las URL de la siguiente etapa están codificadas en la biblioteca XORed con 0x7A.

RECOMENDACIONES.

Según la propia declaración del CEO Nick Galea, la recomendación es desinstalar la aplicación (si está ejecutando Windows Defender, lo hará automáticamente) asimismo, recomienda usar el cliente PWA en su lugar. Este hace el 99% de la aplicación del cliente y está completamente basado en la web, hasta que se lance una nueva versión de la herramienta comprometida.

INDICADORES DE COMPROMISO

INDICADORES DE COMPROMISO.

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:
Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040
WhatsApp: +(502) 5124 9536
Sitio Web: https://www.devel.group/reporta-un-incidente