U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0298

3CX DESKTOP APP COMPROMISED IN SUPPLYCHAIN ATTACK

DATE ISSUED: 31st March 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

A version of the 3CX VoIP (Voice over Internet Protocol) desktop application is compromised as part of a supply chain attack. Once installed, the desktop app pulls malicious files from a Github repository and downloads a previously undetected info-stealer that could steal browser data.

BREAKDOWN

The 3CX app is a private automatic branch exchange (PABX) software that provides several communication functions for its users, including video conferencing, live chat, and call management. Security researchers from SentinelOne and Sophos discovered that the 3CX app download is part of a multi-stage supply chain attack targeting Windows and Mac users. It begins when the MSI installer is downloaded from 3CX's website, loading malicious dynamic link library (DLL) files, ffmpeg.dll and d3dcompiler_47.dll. Next, ffmpeg.dll reads and decrypts the encrypted code from d3dcompiler_47.dll. A decrypted code access icon files (.ico) from GitHub that contain Base64 strings appended to the end of the images. Finally, the Base64 strings have a command and control (2C) server and download an info-stealer malware on the comprised machine. This malware can steal sensitive information and stored credentials from user profiles on Google Chrome, Edge, Brave and Mozilla Firefox browsers. Windows versions 18.12.407,18.12.416, and 18.11.1213 are compromised. Mac versions 18.11.1213, 18.12.402, 18.12.407 & 18.12.416 versions are also infected.

REMEDIATION STEPS

- Organisations can uninstall the 3CX desktop app immediately and switch to the PWA client.
- Install anti-malware software: To protect endpoints from malware, regularly update the agent to detect and block the latest threat.
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.
- Schedule regular malware and vulnerability scans to provide an opportunity to mitigate potential security flaws proactively.

REFERENCES & RESOURCES

The Bleeping Computer	https://www.bleepingcomputer.com/news/security/hackers-compromise-3cx-desktop-app-in-a-supply-chain-attack/amp/
Tenable	https://www.tenable.com/blog/3cx-desktop-app-for-windows-and-macos-reportedly-compromised-in-supply-chain-attack
Sophos	https://community.sophos.com/b/security-blog/posts/3cx-desktop-application-attack