SECURITY ADVISORY

CYBER STASH

March, 2023

CVE-2023-29059

3CX DesktopApp Supply Chain Attack

Context

3CX is an open standard, software-based phone system based on the SIP standard. It works with a range of phone hardware and also features web browser-based extensions and mobile apps. Several cybersecurity vendors expressed concerns on March 29th 2023, about a potential supply chain attack involving tampered 3CX installers that had been digitally signed. The attack aimed to compromise downstream customers. 3CX's CEO confirmed that the desktop app was compromised with malware and advised customers to uninstall it and switch to the Progressive Web App (PWA) client. This new malware impacts the 3CX Windows and macOS desktop app with the ability to gather system information and steal stored credentials and data from user profiles of Chrome, Edge, Brave, and Firefox.

Affected Platform and Versions:

- **Windows**: 18.12.407 & 18.12.416 of the 3CX Desktop App
- **macOS**: 18.11.1213, 18.12.402, 18.12.407, and 18.12.416 of the 3CX Desktop App

Mitigation

To prevent the 3CX Supply Chain Attack and similar incidents, follow these steps:

Upgrade to the latest version of the software: Ensure that you have the most recent version of 3CX installed. This will include security patches and fixes that address vulnerabilities exploited in the attack.

Conduct software updates in a sandbox environment: Before implementing software updates, run them in a controlled sandbox environment. This allows you to observe their behavior and detect any suspicious activities without risking your live system.

Implement application controls: Establish strict controls for how each application interacts with its environment and the internet. Limit access and permissions to prevent unauthorized actions or communications that may compromise the software's security.

Technical Details

Tactics, Techniques and Procedures

The notable TTPs related to the 3CXDesktopApp Supply Chain attack are:

T1055 - Shellcode Execution

The 3CXDesktopApp application serves as a shellcode loader, executing shellcode from heap space.

T1055.001 - Reflective DLL Injection

The shellcode reflectively loads a DLL by removing the "MZ" header. After installation, two malicious DLL files, ffmpeg.dll and d3dcompiler_47.dll, are extracted and used in the next stage

T1055.003 - Exported Function

The loaded DLL is called via a named export, specifically DllGetClassObject. The decrypted shellcode downloads icon files containing Base64 encoded strings from a GitHub repository

T1027 - Obfuscated Files or Information

The ICO files downloaded from the dedicated GitHub repository have base64 encoded data appended after a "$" character.

T1001.001 - Data Obfuscation

The malware searches for the "$" character and extracts the remaining bytes from the ICO file, which are then decoded and decrypted to yield a C&C (Command and Control) URL.

T1043 - Command and Control

The malware establishes communication with the C&C server using the decoded URL and starts its main loop.

T1005 - Data from Local System

The malware gathers information about the victim's computer, including the computer name, domain name, Windows version, and contents of the "config.json" file in the "3CXDesktopApp\config" directory.

T1003 - Credential Dumping

The malware attempts to access the browsing history database of each targeted browser to gather credentials.

References

Related IOC's

https://github.com/sophoslabs/IoCs/blob/master/3CX%20IoCs%202023-03.csv

Public Intelligence

https://www.bleepingcomputer.com/news/security/3cx-confirms-north-korean-hackers-behind-supply-chain-attack/

https://www.zscaler.com/blogs/security-research/3CX-supply-chain-attack-analysis-march-2023

https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/

https://www.virustotal.com/gui/file/7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896

https://www.virustotal.com/gui/file/11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29059

https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/

https://news.sophos.com/en-us/2023/03/29/3cx-dll-sideloading-attack/

https://www.huntress.com/blog/3cx-voip-software-compromise-supply-chain-threats

https://www.fortinet.com/blog/threat-research/3cx-desktop-app-compromised

Act now to protect your business!

Contact CyberStash today to learn about eclipse.xdr and our round-the-clock managed detection and response service.