3CX Desktop App Compromised (CVE-2023-29059)

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

March 30, 2023

FortiGuard Labs Threat Research

By FortiGuard Labs | March 30, 2023

This is a developing story. Please check back for the latest updates from FortiGuard Labs. For a report of this event, please visit our Threat Signal Reports page.

On March 29, a number of reports surfaced that a legitimate signed file from VoIP/IP PBX solutions provider 3CX (3CXDesktop App) had been trojanized due to a code-level compromise. This is the latest high-profile supply chain attack, beginning with SolarWinds and Kaseya a few years ago. This issue has been assigned CVE-2023-29059.

3CXDesktop App is a multi-platform softphone application for desktops (Linux, MacOS, and Windows). The 3CXDesktop App allows users to interact via chat, messaging, video, and voice. Initial reports suggested that all platforms of the 3CXDesktop App were compromised. But at the time of writing, it appears that only the Electron framework versions of MacOS (versions 18.11.1213, 18.12.402, 18.12.407, and 18.12.416) and Windows (versions 18.12.407 and 18.12.416) of the 3CX Desktop App are affected. 3CX has stated that they are working on a new version of the Windows app and have revoked the certificate for the previous version. Initially, there was some confusion about

whether the MacOS version was affected, as the CEO of 3CX issued a statement that only the Windows version of the app was affected. However, this statement was later retracted. Currently, no status on the availability of the MacOS version has been provided at the time of writing.

The company's website boasts that 3CX is available in over 190 countries worldwide, with over 12 million daily users and a 600,000-plus customer base. Companies listed on its website include high-profile organizations in the automobile, aerospace, finance, food and beverage, government, hospitality, and manufacturing sectors, to name a few.

The trojanized 3CX Desktop App is part of a multi-stage attack that utilizes a malicious sideloaded DLL (ffmpeg.dll - SHA256: 7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896) that contains instructions and a payload within another DLL via an encrypted blob (d3dcompiler_47.dll – SHA256: 11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03). This blob also contains the shellcode, which tries to pull ICO files from GitHub (currently down) that contain various URIs for download, where the payload is ultimately loaded and installed to the target environment. However, we could not confirm further details as the repository is currently down.

Discovery of Two 3CXDesktopApp.exes – but Only One Sideloads the Malicious DLL

Looking at the Windows installer (SHA256:aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868), it drops TWO 3CXDesktopApp.exe files.

The SECOND (inside app-18.12.407 folder) is the one that sideloads the ffmpeg.dll file.

C:\Users\Admin\AppData\Local\Programs\3CXDesktopApp\3CXDesktopApp.exe

Filesize: 541KB

MD5: 08d79e1fffa244cc0dc61f7d2036aca9

SHA1: 480dc408ef50be69ebcf84b95750f7e93a8a1859

SHA256: 54004dfaa48ca5fa91e3304fb99559a2395301c570026450882d6aad89132a02

C:\Users\Admin\AppData\Local\Programs\3CXDesktopApp\app-18.12.407\3CXDesktopApp.exe

Filesize: 142MB

MD5: bb915073385dd16a846dfa318afa3c19

SHA1: 6285ffb5f98d35cd98e78d48b63a05af6e4e4dea

SHA256: dde0334807551279624138 9dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc

Figure 1. Ffmpeg.dll starts call to "malicious_payload"

Figure 2. Searching for the FEEDFACE marker

Figure 3. "3jB(2bsG#@c7" string used to decrypt d3dcompiler_47.dll blob

Heatmap - Focus on Europe and North America

Below is a heat map based on recent connections to known malicious domains associated with this attack that FortiGuard Labs observed at the time of writing (March 31st, 2023):

Figure 4. Heat map of the network activities associated with the 3CX supply chain attack

Based on our telemetry, we see that the top 10 countries highlight the geographic spread of victim machines calling out to known actor controlled infrastructure; which appears to target European and North American victims more:

Figure 5. Breakdown of the network activities by country

The following chart reveals a regional breakdown that further proves this point as close to 80 percent of the connections to the attacker controlled infrastructure are concentrated in Europe and North America. This may indicate that the threat actor is mainly targeting enterprises in those regions – however, this is uncertain. This could be indicative of 3CX product's geographic customer base - including the possibility of various multinational corporations operating inside those regions.

Figure 6. Regional breakdown of 3CX network activities

What Mitigations Are Available?

3CX suggests that users migrate to the PWA app in the meantime. The PWA app is web-based and is unaffected by the supply chain attack. Customers on 3CXHosted and StartUP are not affected. Additional details on updates and best practices can be found here. FortiGuard Labs suggests that all older variants of the 3CX Desktop App be discontinued immediately until newer unaffected versions are available.

What is the Status of Coverage?

Fortinet Customers running the latest definitions are protected by the following AV signatures:

W64/Agent.CFM!tr

OSX/Agent.CN!tr

Riskware/Sphone_XC3

All known network IOCs related to this attack are blocked by the WebFiltering client. For a detailed overview of all Fortinet protections for this event, please visit our Outbreak Alerts page.

Indicators of Compromise (IOCs)	Hash	Detections
aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868	SHA2	Riskware/Sphone_XC3
59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983	SHA2	Riskware/Sphone_XC3
92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61	SHA2	Riskware/Sphone_XC3
5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290	SHA2	OSX/Agent.CN!tr
b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb	SHA2	Riskware/Sphone_XC3
e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec	SHA2	Riskware/Sphone_XC3
11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03	SHA2	W64/Agent.CFM!tr
7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896	SHA2	Riskware/Sphone_XC3

c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02	SHA2	Riskware/Sphone_XC3
b5e318240401010e4453e146e3e67464dd625cfef9cd51c5015d68550ee8cc09	SHA2	W64/Agent.CFM!tr
aa4e398b3bd8645016d8090ffc77d15f926a8e69258642191deb4e68688ff973	SHA2	W64/Sphone_XC3.INFS!tr.dldr
a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67	SHA2	Riskware/Sphone_XC3
dde03348075512796241389dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc	SHA2	Riskware/Sphone_XC3
fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405	SHA2	Riskware/Sphone_XC3

FortiEDR detects installation of the 3CX Desktop App with a dynamic code exception event:

FortiEDR also blocks the final payload making a network connection to C2:

FortiGuard Labs has released a new Application Control signature that will detect attempted 3CX access activity which was released in definitions set (23.528):

3CX

Regarding FortiAnalyzer, a knowledge base article that contains detailed insight on how to detect activities related to the 3CX Supply Chain attack can be found here.

Network IOCs

akamaicontainer[.]com

akamaitechcloudservices[.]com

azuredeploystore[.]com

azureonlinecloud[.]com

azureonlinestorage[.]com

dunamistrd[.]com

glcloudservice[.]com

journalide[.]org

msedgepackageinfo[.]com

msstorageazure[.]com

msstorageboxes[.]com

officeaddons[.]com

officestoragebox[.]com

pbxcloudeservices[.]com

pbxphonenetwork[.]com

pbxsources[.]com

qwepoi123098[.]com

sbmsa[.]wikisourceslabs[.]com

visualstudiofactory[.]com

zacharryblogs[.]com

azureonlinestorage.com

convieneonline[.]com

Soyoungjun[.]com

Related Posts