National Cyber Security Centre

2303300115-NCSC

A part of the **Department of the Environment, Climate & Communications**

# NCSC Alert

## 3CX Supply Chain Compromise

Friday 31st March, 2023

**STATUS:** TLP-CLEAR

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use* TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

## Description

The NCSC has been made aware of a digitally signed and trojanized version of the 3CX VOIP desktop client, DesktopApp.exe. 3CX is a software-based PBX system available across multiple platforms. The supply chain attack affects their Electron Windows App in Update 7, versions 18.12.407 and 18.12.416 and Electron Mac App versions 18.11.1213, 18.12.402, 18.12.407 and 18.12.416.

According to a blog post from 3CX, the supply chain attack is due to bundled libraries compiled via GIT. The binary 3CXDesktopApp.exe is the first stage in a multi-stage attack, that loads two additional malicious payloads, ffmpeg.dll and d3dcompiler_47.dll. The decrypted code then attempts to download .ICO files with BASE64 code appended to them. This BASE64 code contains the C2 domains required for additional payloads. At the time of writing a number of the domains as well as the GitHub page have been taken down.

Anti-Virus vendors have been detecting malicious activity related to this campaign as early as the 22nd of March 2023, with infrastructure related to the campaign registered in December of 2022.

## Products Affected

- Electron Windows App shipped in Update 7, versions :
  - 18.12.407
  - 18.12.416
- Electron Mac App versions:
  - 18.11.1213
  - 18.12.402
  - 18.12.407
  - 18.12.416

## Impact

The malware dropped acts as Infostealer, harvesting system information, data and stored credentials from browser user profiles. This information is likely to be leveraged in future campaigns. There have been some reports of hands-on activity from the Threat Actor in certain instances.

## Recommendations

The NCSC recommends that organisations remove the compromised software and patch once the update becomes available. Threat hunting activities should be initiated by security on known IOCs. Please see the SophosLabs Github repository. The security researcher Florian Roth has also generated YARA rules to help detect activity related to this campaign.

The 3CX security alert advises customers to use the PWA App as it is completely web and it does not require any installation or updating.

A number of AV vendor solutions have already enabled protections against this campaign and known IOCs. Please consult with your security provider for further information.

**DISCLAIMER:** This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
**Tel:** +353 (0)1 6782333
**Mail:** certreport@decc.gov.ie
**Web:** ncsc.gov.ie
**Twitter:** ncsc_gov_ie
**LinkedIn:** ncsc-ie