Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Active Campaign Targeting VOIP IPBX 3CX DesktopApp

Date of Issue: 06 April 2023

Severity Level: High

System Affected:

- 3CX version 18.12.407 and 18.12.416 for Windows
- 3CX version 18.11.1213, 18.12.402, 18.12.407, and 18.12.416 for MacOS.

Description:

Voice Over IP (VOIP) IPBX software development company 3CX has fallen victim to a supply chain cyberattack. Consequently, the recent versions of 3CX DesktopApp have been reportedly compromised by an advanced persistent threat group and malicious versions of the software have been distributed to customers. As part of this supply chain attack, two DLLs used by the Windows desktop application were replaced with malicious versions that download additional malware to computers, such as an information-stealing Trojan. Attackers could leverage the malicious applications to perform further malicious activity including the remote deployment of second stage malware. It is to be noted that the 3CX phone system is used by more than 600,000 companies across the world, and 12 million users worldwide.

Telemetry data shared by Security firm Fortinet shows that the geographic spread of victim machines calling out to known actor controlled infrastructure chiefly spans Italy, Germany, Austria, the U.S., South Africa, Australia, Switzerland, the Netherlands, Canada, and the U.K.

CERT-MU strongly advises Internet Service Providers, telecommunication operators and other organisations using the 3CX VOIP software to watch out for this vulnerability and apply remedial actions according.

Workarounds:

The company 3CX stated that it is engaging the services of Google-owned Mandiant to review the incident. Affected organisations are required to immediately uninstall affected versions of 3CX DesktopApp. The software development company 3CX have advised that they are looking to publish an updated version of their Windows client, and that their Web Client or Progressive Web Application (PWA) can be used as an alternative. More information is available on:

https://www.3cx.com/user-manual/web-client/

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication and Innovation
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org