OUTBREAK ALERTS

3CX Supply Chain Attack

3CX VoIP DesktopApp Campaign & Supply Chain Threats

https://www.3cx.com/blog/news/desktopapp-security-alert/
CVEs: CVE-2023-29059

Security researchers observed that the threat actors abused a popular business communication software by 3CX. The reports mention that a version of the 3CX VoIP (Voice over Internet Protocol) desktop client was trojanized and is being used to attack multiple organizations.

Background

3CXDesktopApp is a voice and video conferencing Private Automatic Branch Exchange (PABX) enterprise call routing software developed by 3CX, a business communications software company. The company website claims that 3CX has 600,000 customers and over 12 million daily users. 3CX customers are in multiple sectors such as automotive, hospitality, food & beverage, Managed Information Technology Service Provider (MSP) and manufacturing.

According to the vendor, "this appears to have been a targeted attack from an Advanced Persistent Threat, perhaps even state sponsored, that ran a complex supply chain attack." Due to widespread usage of the software across different sectors and organizations, this has the potential to be a massive supply chain attack similar to what we have seen in the past like SolarWinds incident or the Kaseya VSA ransomware attack.

Announced

March 30th, 2023: 3CX posted an alert at:
https://www.3cx.com/blog/news/desktopapp-security-alert/

March 30th 2023: CISA released an alert at:
https://www.cisa.gov/news-events/alerts/2023/03/30/supply-chain-attack-against-3cxdesktopapp

Latest Developments

FortiGuard Labs has released updated Antivirus definitions and blocked all the known IoCs including Domains, C2 servers and IPs related to the attack. FortiGuard AI/ML engine is able to prevent and block download of malware payload automatically without any human intervention.

FortiGuard Labs is continually monitoring the situation and will provide new information as it becomes available.

Apr 27, 2023. Critical Infrastructure Organizations Compromised through Trojanized X_Trader Software
https://www.fortiguard.com/threat-signal-report/5192

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery

AV

Blocks malware related to 3CX Supply Chain Attack

FortiGate *DB 91.01895* | FortiClient *DB 91.01895* | FortiSASE *DB 91.01895* | FortiMail *DB 91.01895* | FortiCASB *DB 91.01895* | FortiCWP *DB 91.01895* | FortiADC *DB 91.01895* | FortiProxy *DB 91.01895*

App Control

Provides visibility into 3CX application usage in real time on the network

FortiGate *DB 23.528*

Vulnerability

Detects installed malicious version of 3CX DesktopApp

FortiClient *DB 1.432*

AV (Pre-filter)

Blocks malware related to 3CX Supply Chain Attack

FortiEDR *DB 91.01895* | FortiSandbox *DB 91.01895* | FortiNDR *DB 91.01895*

Behavior Detection

Blocks malware based on Community Cloud Query

FortiSandbox *v4.0+*

- Exploitation

IPS

Detects and Blocks 3CX DesktopApp Supply Chain Backdoor traffic

FortiGate *DB 23.526* | FortiSASE *DB 23.526* | FortiNDR *DB 23.526* | FortiADC *DB 23.526* | FortiProxy *DB 23.526*

Web App Security

Detects and Blocks 3CX DesktopApp Supply Chain Backdoor traffic

FortiWeb *DB 3.00547*

Pre-execution

Behavior Dectection Engine prevents the malicious app from downloading the 3CX payload

FortiEDR *v5.0+*

- Installation

Web Filter

Blocks known IOCs related to 3CX Supply Chain Attack

FortiGate *DB 27.21239*

Post-execution

Behavior Dectection Engine detects and blocks malicious activities related to 3CX Attack

FortiEDR *v5.0+*

- C2

Botnet C&C

Blocks known C2 servers related to 3CX Supply Chain Attack

FortiGate *DB 3.00219*

- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiClient *DB 1.10* | FortiAnalyzer *DB 1.00097*

Threat Hunting

FortiEDR *v4.0+* | FortiAnalyzer *v6.4+* | FortiSIEM *v6.6+*

IOC

Blocks known IOCs related to 3CX Supply Chain Attack

FortiAnalyzer | FortiSIEM | FortiSOCaaS

Content Update

FortiSIEM *DB 313*

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response | FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

Security Rating | FortiRecon: EASM

Additional Resources

FortiGuard Threat Signal	https://www.fortiguard.com/threat-signal-report/5192/
CISA Alert	https://www.cisa.gov/news-events/alerts/2023/03/30/supply-chain-attack-against-3cxdesktopapp
Security Week	https://www.securityweek.com/3cx-confirms-supply-chain-attack-as-researchers-uncover-mac-component/
The Hacker News	https://thehackernews.com/2023/03/3cx-desktop-app-targeted-in-supply.html
Bleeping Computer	https://www.bleepingcomputer.com/news/security/hackers-compromise-3cx-desktop-app-in-a-supply-chain-attack/

Learn more about FortiGuard Outbreak Alerts