NFIR Threat Intelligence Report

Supply chain attack op softwarepakket 3CX versie 7

Datum: 31/03/2022
Versie: 1.0

Beschrijving

Op 30 maart heeft Cybersecuritybedrijf CrowdStrike[1] aangegeven een digitale aanval op gebruikers van het softwarepakket 3CX te hebben waargenomen. Deze aanval wordt ook wel een supply chain attack genoemd – waarbij de distributie en/of update-kanalen van een softwareleverancier misbruikt worden om malafide software te verspreiden.

3CX is een veelgebruikte en uitgebreide Voice-over-IP (VoIP) softwareoplossing voor bedrijven, die onder andere wordt gebruikt door telefooncentrales. NFIR adviseert gebruikers van deze software om direct actie te ondernemen. De aanval heeft het CVE-nummer CVE-2023-29059[2] toegewezen gekregen.

De getroffen versies van het 3CX VoIP-product betreffen tenminste de volgende:

Product	Platform
3CX versie 18.12.407 3CX versie 18.12.416	Electron Windows
3CX versie 18.11.1213	Electron MacOS 18.11
3CX versie 18.12.402 3CX versie 18.12.407 3CX versie 18.12.416	Electron MacOS 18.12

Tabel 1: Overzicht van de getroffen producten

NFIR adviseert om vast te stellen of de malafide versies van 3CX zoals hierboven beschreven aanwezig zijn op systemen binnen uw organisatie. De malafide versies worden verspreid door een malafide stuk software in 3CX Desktop-App update 7. Deze update is volgens 3CX sinds eind maart 2023 beschikbaar. Indien u een besmette versie constateert adviseert NFIR om incident response & digitaal forensisch onderzoek uit te voeren.

> Accuut hulp nodig? Bel dan onze 24/7 CERT-lijn via 088 133 0700 en wij doen ons uiterste best om u zo snel mogelijk te helpen.

[1] https://www.crowdstrike.com/blog/CrowdStrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/
[2] https://nvd.nist.gov/vuln/detail/CVE-2023-29059

Hoe stel ik vast of 3CX gebruikt wordt binnen mijn organisatie?

Het is middels de volgende commando's mogelijk om de aanwezigheid vast te stellen van 3CX op apparaten binnen uw organisatie:

Windows-systemen

```
# Controle of er een actief proces is gerelateerd aan 3CX
Get-WmiObject -Class Win32_Process -Filter "Name='3CXDesktopApp.exe'"

# Controle op Windows-register
Get-ItemProperty -Path
'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*' -ErrorAction
SilentlyContinue | Where-Object { $_.DisplayName -like '3CX Desktop App' }

# Controle op de 3CX gebruikersprofielen
Test-Path -Path C:\Users\*\appdata\local\programs\3cxdesktopapp\
```

MacOS-systemen

```
# Controle op aanwezigheid van programma op MacOS in /Applications
ls '/Applications' | grep '3CX'

# Controle op aanwezigheid van een map binnen Application support folder
if [ -d /Users/*/Library/Application\ Support/3CX\ Desktop\ App/ ]; then echo
"3CXDesktop exists"; fi
```

Hoe blokkeer ik de installatie van de gehackte 3CX-softwareversies binnen mijn organisatie?

NFIR adviseert om de volgende bestandshashes toe te voegen aan de deny-list van uw anti-virus/malware of EDR-oplossing om installatie van de (bekende) malafide 3CX versies te voorkomen:

SHA-256 hash	Platform	SHA-256 hash (installer)	Bestandsnaam
dde033480755127962413 89dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc	Windows	aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868	3cxdesktopapp-18.12.407.msi
fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405	Windows	59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983	3cxdesktopapp-18.12.416.msi
92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61	macOS	5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290	3CXDesktopApp-18.11.1213.dmg
b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb	macOS	e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec	3cxdesktopapp-latest.dmg

Hoe detecteer ik mogelijk misbruik binnen mijn organisatie?

Op basis van de publiek beschikbare informatie zijn in ieder geval de volgende malafide domeinnamen geidentificeerd:

Domeinnamen	
akamaicontainer[.]com	msedgepackageinfo[.]com
akamaitechcloudservices[.]com	msstorageazure[.]com
azuredeploystore[.]com	msstorageboxes[.]com
azureonlinecloud[.]com	officeaddons[.]com
azureonlinestorage[.]com	officestoragebox[.]com
dunamistrd[.]com	pbxcloudeservices[.]com
glcloudservice[.]com	pbxphonenetwork[.]com
qwepoi123098[.]com	zacharryblogs[.]com
sbmsa[.]wiki	pbxsources[.]com
sourceslabs[.]com	journalide[.]org
visualstudiofactory[.]com	

NFIR adviseert om de bovenstaande domeinnamen binnen IDS/IPS/EDR-oplossingen te configureren als detectieregel. Het betreft een lopende actuele situatie waarbij nieuwe indicatoren van een infectie beschikbaar kunnen komen. Als u vermoed getroffen te zijn door deze supply-chain aanval adviseert NFIR u om incident response & forensisch onderzoek te laten doen naar of uw systemen getroffen zijn.

Actieplan

Het is belangrijk voor uw organisatie om ten minste de volgende stappen te nemen:

1. Controleer de publiek beschikbare Indicators-of-Compromise (IoC's) op uw systemen om vast te stellen of er systemen mogelijk gecompromitteerd zijn, of laat extern preventief onderzoek uitvoeren naar uw systemen.
2. In navolging op het advies van het NCSC[3] adviseert NFIR om de malafide versies van de 3CX software te verwijderen en te wachten tot er een 'veilige' versie door de software-leverancier wordt gepubliceerd – in de tussentijd adviseert 3CX om gebruik te maken van de PWA-variant van de applicatie - 3CX Security Alert for Electron Windows App | Desktop App.
3. Indien uw organisatie gebruikmaakt van 3CX adviseert NFIR om altijd forensisch onderzoek uit te laten voeren om vast te stellen of uw omgeving gecompromitteerd is.

Heeft u systemen waarvan het risico groot is (bijvoorbeeld systemen met zeer gevoelige of bijzondere persoonsgegevens)? Zo ja, heeft u mogelijk indicaties dat het systeem niet direct gemitigeerd en/of geüpdatet kan worden? Overweeg dan om het systeem tijdelijk uit te schakelen totdat deze geüpdatet kan worden.

[3] https://www.ncsc.nl/actueel/nieuws/2023/maart/30/ncsc-waarschuwt-voor-supplychain-aanval-3cx

Wat moet mijn organisatie doen als mijn organisatie getroffen is?

Als uw organisatie vermoedelijk slachtoffer is geworden van deze aanval, is het dringende advies om onderzoek uit te laten voeren naar de toedracht, in hoeverre aanvallers mogelijk andere systemen hebben gecompromitteerd en welke informatie mogelijk ongeautoriseerd geraadpleegd is.

1. Koppel indien mogelijk de getroffen systemen los van het netwerk, maar laat deze aanstaan (in verband met eventuele sporen zoals het vluchtige geheugen – RAM);
2. Laat de getroffen systemen forensisch onderzoeken;
3. Zorg voor adequate back-ups;
4. Reset uw wachtwoorden en gebruikersgegevens;
5. Doe aangifte bij de Politie;
6. Overweeg een melding te doen bij de Autoriteit Persoonsgegevens.

Heeft uw organisatie op dit moment een incident? Onze Computer Emergency Response Teams (CERT) staan 24/7 voor organisaties klaar om te ondersteunen bij IT- Security Incidenten.

> Accuut hulp nodig? Bel dan onze 24/7 CERT-lijn via 088 133 0700 en wij doen ons uiterste best om u zo snel mogelijk te helpen.

Over NFIR

NFIR is een specialist in cyberbeveiliging. Bij NFIR zijn cyber-engineers in dienst: Hackers die weten wat ze doen, testers die de werking van ICT-infrastructuren en software begrijpen, privédetectives die, indien nodig, onderzoeken kunnen uitvoeren en adviseurs/consultants die u het juiste advies kunnen geven of die u kunnen ondersteunen bij een incident.

Gespecialiseerd in

- Het verzamelen, identificeren en valideren van digitale informatie
- Onderzoek naar computers, servers, e-mailverkeer, gegevensdragers, websites en personen

Multidisciplinair onderzoek

- Sporen en gegevens verzamelen en reconstrueren
- Heldere rapportage bruikbaar voor juridische procedures en andere officiële instanties

Samenwerking met

- Tactisch rechercheurs, privacy juristen, gerechtsdeurwaarders, Politie, NCSC, IBD, het Openbaar Ministerie en internationale diensten.

NFIR als adviseur Forensisch Onderzoek

- Samen met de opdrachtgever wordt de scope van het onderzoek bepaald
- Praktisch toepasbare adviezen na afronding van het onderzoek

NFIR B.V.
Verlengde Tolweg 2
2517 JV Den Haag
Telefoon: 088 - 323 02 05
info@nfir.nl
https://www.nfir.nl