Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

Schadhafte Version der 3CX Desktop App im Umlauf

Nr. 2023-214778-1122, Version 1.1, 05.04.2023

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 29. März 2023 berichteten verschiedene Quellen darüber, dass sich eine kompromittierte Fassung des Voice over IP (VOIP)-Clients 3CX Desktop App im Umlauf befinde [SEN2023], [SOP2023]. Die Software ist zwar durch den Hersteller signiert, enthält jedoch schadhafte Elemente, die der Funktion eines Trojaners entsprechen. Grund dafür ist eine manipulierte DLL-Datei. Unter anderem wurde beobachtet, dass die Anwendung nach erfolgreicher Installation eine Verbindung zu einem Command and Control-Server (C&C-Server) aufbaut und weitere Schadsoftware nachlädt. Hieraus folgte zum Beispiel die Installation einer Shell bei den Opfern, mit deren Hilfe die Täter weitere Befehle absetzen können.

Eine Liste der genutzten C&C-Server kann [CRO2023] entnommen werden.

3CX hat die Berichte zwischenzeitlich bestätigt und stellt frühestens für Freitag, den 31. März 2023 ein bereinigtes Release in Aussicht [3CX2023]. Weiterhin nennt das Unternehmen konkret betroffene Produkte. Demnach handele es sich um die folgenden Desktop Apps:

- für Windows: die Versionen 18.12.407 und 18.12.416
- für Mac: die Version 18.11.1213, 18.12.402, 18.12.407 und 18.12.416

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Ein Patch steht zum aktuellen Zeitpunkt nicht zur Verfügung. Auch ergänzende Informationen, wie Kritikalitätsbewertungen nach dem Common Vulnerability Scoring System (CVSS) oder eine eindeutige Nummer nach den Common Vulnerabilities and Exposures (CVE) liegen derzeit nicht vor.

Update 1:
Der Hersteller wiederholte in weiteren Veröffentlichungen nochmals die grundsätzliche Empfehlung, die nativen Anwendungen für Windows und Mac zu deinstallieren und stattdessen die Browser App zu nutzen [3CX2023b], [3CX2023c]. Weiterhin wurde mit einem neuen Zertifikat eine neue Version der Electron Windows App generiert, die derzeit durch ein Sicherheitsunternehmen geprüft wird und in Kürze zum Download bereitgestellt werden soll.

3CX bietet außerdem ein Tool an, mit dem geprüft werden kann, ob zwischenzeitlich eine Kompromittierung von Systemen stattgefunden hat [3CX2023d].

Auch die unter [CRO2023], [SEN2023] und [SOP2023] verlinkten Artikel zum Sachverhalt wurden zwischenzeitlich aktualisiert und um weitere Erkenntnisse ergänzt.

Bewertung

Mithilfe der Tarnung als legitime Software ermöglichen es Supply-Chain-Angriffe – wie der hier beschriebene – den Akteuren im Cyber-Raum innerhalb kurzer Zeit, zahlreiche Netzwerke zu kompromittieren.

Über die Fokussierung auf VoIP-Lösungen lassen sich dabei verschiedene Angriffsszenarien realisieren, wie z.B. das Mithören von Gesprächen oder die Ausweitung des Angriffs auf zusätzliche Netzwerkkomponenten.

Mögliche Auswirkungen auf Kritische Infrastrukturen inkl. Verwaltung

Der geschilderte Vorfall kann auch Kritische Infrastrukturen treffen und die dargestellten Konsequenzen haben.

Fragen an IT-Sicherheitsverantwortliche

- Welche Version der 3CX Desktop App ist in der eigenen Organisation derzeit im Einsatz?
- Kann der 3CX Installer auf dem 3CX-Server (/var/lib/3cxpbx/Instance1/Data/Http/electron/windows/) bis zu einem neuen Release entfernt werden?
- Ist es zusätzlich möglich, ein erneutes Laden des Installers an der Firewall zu blockieren?
  Wurde der automatische 3CX Upgrade-Service gestoppt?
- Ist der Zugriff auf Domains, die mit den Angriffen in Verbindung stehen, unterbunden? [CRO2023]
- Haben Sie die 3CX Desktop App entfernt und nutzen stattdessen wie von diesem empfohlen die PWA App des Herstellers? [3CX2023]
- Haben Sie Maßnahmen veranlasst, um eine bereits erfolgte Kompromittierung des Netzwerks auszuschließen? Wurden zum Beispiel Log-Dateien oder SIEM-Daten analysiert? [BSI2023a]
  Wurden dabei auch die Angriffsindikatoren unter [CRO2023] bei der Analyse berücksichtigt?
- Weil eine zusätzliche Kompromittierung nicht ausgeschlossen werden kann: Sind in der Organisation weitere Komponenten von 3CX im Einsatz?
- Wurden die Hinweise des BSI IT-Grundschutzes berücksichtigt? [BSI2023b], [BSI2023c]

IT-Sicherheitsverantwortliche sollten regelmäßig prüfen, wann der Hersteller auf seiner Webseite eine neue - nicht-kompromittierte - Version der 3CX Desktop App zur Verfügung stellt und diese kurzfristig installieren.

Update 1:
Weiterhin sollten IT-Sicherheitsverantwortliche prüfen, ob die Installation und Ausführung von Anwendungen generell nach Erlaubtlisten-Prinzip über eine Ausführungskontrolle (Application Restriction) eingeschränkt werden

kann. Zertifikaten, die zur Signierung der kompromittierten ausführbaren Dateien verwendet worden sind, sollte darüber hinaus das Vertrauen entzogen werden.

Auch die Möglichkeit zur Nutzung des von 3CX bereitgestellten Tools [3CX2023d] sollte durch IT-Sicherheitsverantwortliche eigenverantwortlich überprüft werden.

Außerdem sollte überprüft werden, ob auch die neuen, unter [CRO2023], [SEN2023] und [SOP2023] ergänzten IoCs zur Detektion von potenziellen Angriffen genutzt werden können.

Im Malware Information Sharing Portal (MISP) wurde ein Event erstellt, das die aktuellen Indicators of Compromise (IoCs) umfasst. Diese können unter der UUID 4589a989-33b3-4b17-bc66-518fb2c258fe eingesehen werden.
Falls Sie weitere Informationen zu MISP benötigen, wenden Sie sich bitte an die für Sie zuständige Kontaktstelle im BSI.

Links

[3CX2023] 3CX DesktopApp Security Alert:
https://www.3cx.com/blog/news/desktopapp-security-alert/

[3CX2023b] Update zum Sicherheitsvorfall: Samstag, 1. April 2023:
https://www.3cx.de/blog/update-zum-sicherheitsvorfall-samstag-1-april-2023/

[3CX2023c] Wählen Sie PWA oder Windows Legacy App statt Electron:
https://www.3cx.de/blog/pwa-vs-windows-legacy-app/

[3CX2023d] Forensic Scanner Nextron THOR:
https://www.3cx.com/community/threads/forensic-scanner-nextron-thor.120005/

[BSI2023a] Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf

[BSI2023b] BSI IT-Grundschutz Edition 2023 – NET.4.2: VoIP:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_4_2_VoIP_Edition_2023.pdf

[BSI2023c] BSI IT-Grundschutz Edition 2023 – APP.6: Allgemeine Software:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_6_Allgemeine_Software_Edition_2023.pdf

[CRO2023] CrowdStrike Falcon Platform Detects and Prevents Active Intrusion Campaign Targeting 3CXDesktopApp Customers:
https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/

[SEN2023] Ongoing Campaign Trojanizes 3CXDesktopApp in a Supply Chain Attack:
https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/

[SOP2023] 3CX users under DLL-sideloading attack: What you need to know:
https://news.sophos.com/en-us/2023/03/29/3cx-dll-sideloading-attack/

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**
  Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
  Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

  TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
  Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**
  Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.