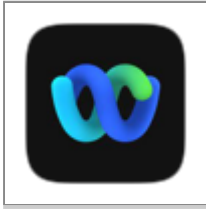


Nieuws



Szabó: rijksoverheid heeft geen geschikt alternatief voor Cisco Webex

woensdag 11 september 2024, 12:38 door [Redactie](#), 8 [reacties](#)

De Rijksoverheid heeft geen geschikt alternatief voor Cisco Webex, zo heeft staatssecretaris Zsolt Szabó voor Digitalisering laten weten op vragen uit de Tweede Kamer. PVV, Nieuw Sociaal Contract (NSC) en de VVD wilden opheldering over het recente **datalek** bij de **videovergaderingsdienst**, waardoor metadata van overheidsvergaderingen voor onbevoegden toegankelijk was. Ook werd er gevraagd naar een opensource-alternatief voor Webex en de manier waarop Cisco met kwetsbaarheden en bugmeldingen omgaat.

Volgens de staatssecretaris werd het datalek bij Webex veroorzaakt doordat er gebruik werd gemaakt van voorspelbare url's. "Dit betrof geen configuratiefout van de Rijksvideodienst (Belastingdienst). De inrichting is gecheckt in samenwerking met CIO Rijk en de AIVD/NBV. Hiervoor is onder andere een BSPA1 en DPIA2 uitgevoerd. Wel kon er via enumeratie, door een voorspelbare logische volgordelijkheid in de unieke internetadressen van websites (URL's genoemd), metadata van andere vergaderingen worden ingezien door ongeautoriseerde gebruikers."



Cisco heeft laten weten dat dit mogelijk was door kwetsbaarheden in specifiek de Cloud-applicaties van Cisco Webex meetings. "De Rijksoverheid heeft aanbevolen veiligheidsinstellingen en werkt veelal niet met de cloudversie, maar met de clientversie van Webex", voegt Szabó toe. Het bleek ook mogelijk dat ongeautoriseerde gebruikers onder bepaalde voorwaarden vertrouwelijke videovergaderingen hebben kunnen bijwonen. Cisco ondersteunt namelijk de mogelijkheid in te bellen via het Public Switched Telephone Network op Cisco Webex Meetings. In Nederland zijn echter geen gevallen hiervan bekend, aldus de staatssecretaris.

Overleg met Cisco over CVD-beleid

PVV-Kamerlid Valize, NSC-Kamerlid Six Dijkstra en VVD-Kamerlid Rajkowski hadden ook vragen gesteld over het 'coordinated vulnerability disclosure' (CVD)-beleid van Cisco. Via dergelijk beleid geven organisaties aan hoe ze met meldingen van kwetsbaarheden omgaan. "Cisco heeft ervoor gekozen om in dit geval een andere procedure dan de coordinated vulnerability disclosure (CVD) procedure te volgen en geen kenmerken toe te kennen aan de kwetsbaarheden", laat Szabó weten. "Naar aanleiding van het incident wordt op korte termijn overleg met Cisco gevoerd om Cisco's beleid en processen ten aanzien van mogelijke toekomstig geconstateerde kwetsbaarheden/incidenten aan te passen."

Alternatief

Als laatste hadden de Kamerleden gevraagd of de staatssecretaris bereid is om een opensource-alternatief voor Webex te overwegen. "De selectie van een leverancier voor het rijksbreed videoconferencing platform heeft middels een openbare aanbesteding plaatsgevonden. Geen van de inschrijvende partijen had een open source oplossing aangeboden", antwoordt Szabó. "Uiteraard houden wij ons graag op de hoogte van de ontwikkelingen in de markt, maar we zien dat wat betreft de schaalgrootte en de complexiteit van de organisatie van de rijksoverheid er op dit moment geen gelijkwaardige alternatieven beschikbaar zijn."

-  [Ict-bedrijf aansprakelijk voor schade van ransomware-aanval bij klant](#)
-  [Britse overheid roept bedrijven op om datalekken en cyberaanvallen te melden](#)

Reacties (8)

11-09-2024, 13:01 door Anoniem

[Reageer met quote](#) 

<https://jitsi.org/>

11-09-2024, 13:05 door Anoniem

[Reageer met quote](#) 

"De Rijksoverheid heeft aanbevolen veiligheidsinstellingen en werkt veelal niet met de cloudversie, maar met de clientversie van Webex"

Oh maar dat is nog erger, want die download bij opstarten executable files van internet naar user-writable storage en voert die vervolgens uit.
Bij fatsoenlijke instellingen van je werkstation wordt dat niet toegestaan, en daar moeten dan uitzonderingen op worden gemaakt voor Webex, wat het systeem als geheel onveiliger maakt. Met name risico voor allerlei ongewenste RAT en ander malware.

11-09-2024, 13:28 door Anoniem

[Reageer met quote](#) 

Cisco heeft stnadaard backdoors / fixed usernames in hard en software. Verplicht door NSA.
Antwoord Cisco bij bevinding: wij mogen hier niets over zeggen.

11-09-2024, 16:13 door Anoniem

[Reageer met quote](#) 

Door Anoniem: "De Rijksoverheid heeft aanbevolen veiligheidsinstellingen en werkt veelal niet met de cloudversie, maar met de clientversie van Webex"

Oh maar dat is nog erger, want die download bij opstarten executable files van internet naar user-writable storage en voert die vervolgens uit.
Bij fatsoenlijke instellingen van je werkstation wordt dat niet toegestaan, en daar moeten dan uitzonderingen op worden gemaakt voor Webex, wat het systeem als geheel onveiliger maakt. Met name risico voor allerlei ongewenste RAT en ander malware.

Je zal toch wel begrijpen dat er geen executable files van internet gedownload en geïnstalleerd worden.
Maar nee, gelijk een oordeel vellen over een zelfverzonnen situatie bij de overheid die totaal niet klopt.

11-09-2024, 16:57 door Anoniem

[Reageer met quote](#) 

Door Anoniem:

Door Anoniem: "De Rijksoverheid heeft aanbevolen veiligheidsinstellingen en werkt veelal niet met de cloudversie, maar met de clientversie van Webex"

Oh maar dat is nog erger, want die download bij opstarten executable files van internet naar user-writable storage en voert die vervolgens uit.
Bij fatsoenlijke instellingen van je werkstation wordt dat niet toegestaan, en daar moeten dan uitzonderingen op

Zoeken



Vacature



Rijksoverheid

Information Security Officer (ISO)

Dienst Justitiële Inrichtingen

Ben jij een tech-liefhebber met een passie voor informatiebeveiliging? Wil je jouw expertise inzetten om de veiligheid te waarborgen binnen een dynamische omgeving? Dan is de rol van Informatiebeveiligingsfunctionaris bij Justitieel Complex Zaanstad wellicht jouw volgende avontuur! In deze rol ben jij de sleutel tot het creëren en handhaven van een veilige werkomgeving, waarbij onze organisatie optimaal blijft draaien.

[Lees meer](#) 

Privacyvriendelijke leeftijdsverificatie:

- ☐ Kansloos
- ☐ Het proberen waard
- ☐ ' OR '1'='1

Aantal stemmen: **943** [17 reacties](#)

Vacature



Gemeente Utrecht

Chief Information Security Officer

Utrecht heeft jou nodig! Als Chief Information Security Officer speel jij een cruciale rol in de bescherming van de digitale informatie van de gemeente Utrecht. Als geen ander weet jij welke dreigingen er zijn en kun je deze vertalen naar risico's die de gemeente en haar inwoners lopen. Solliciteer nu!

[Lees meer](#) 



Vacature

SECURITY CHALLENGES



Cybersecurity Trainer / Streamer

Toe aan een nieuwe nieuwe job waarmee je het verschil maakt? In de Certified Secure trainingen laat je deelnemers zien hoe actuele kwetsbaarheden structureel verholpen worden. Ook werk je actief mee aan de ontwikkeling van onze gamified security challenges. Bij het maken van challenges kom je telkens nieuwe technieken tegen, van Flutter tot GraphQL, van Elastic Search tot Kubernetes.

[Lees meer](#) 

Security.NL - X

10-01-2024 door [Redactie](#)

worden gemaakt voor Webex, wat het systeem als geheel onveiliger maakt. Met name risico voor allerlei ongewenste RAT en ander malware.

Je zal toch wel begrijpen dat er geen executable files van internet gedownload en geïnstalleerd worden. Maar nee, gelijk een oordeel vellen over een zelfverzonnen situatie bij de overheid die totaal niet klopt.

Je kent Webex kennelijk niet!
Dit is een programma wat je wel kunt installeren op een computer, maar als je het dan opstart download het meteen weer extra code en die voert het dan uit.
Dus als je gebruikers helemaal verbiedt om code te downloaden en uit te voeren dan werkt de Webex client niet! (wel de webversie)
Dit is geen zelfverzonnen situatie hoor, dit is gewoon eigen ervaring.

Altijd meteen op de hoogte van het laatste security nieuws? Volg ons ook op X!

[Lees meer](#)

12-09-2024, 11:01 door [Drs Security en Privacy](#) [Reageer met quote](#)

Fijn dat de rijksoverheid, ministereis op eigen houtje, allemaal Microsoft teams aan het implementeren zijn waarbij Microsoft gewoon de master key heeft.
Bij Webex kun je, als je dat wil en instelt, tenminste gewoon de meeting in end2end encryptie modus zetten en dan ook nog de sleutels zelf beheren zodat Cisco helemaal niets meer kan.

12-09-2024, 11:04 door [Drs Security en Privacy](#) [Reageer met quote](#)

Door Anoniem:

Door Anoniem:

Door Anoniem: "De Rijksoverheid heeft aanbevolen veiligheidsinstellingen en werkt veelal niet met de cloudversie, maar met de clientversie van Webex"

Oh maar dat is nog erger, want die download bij opstarten executable files van internet naar user-writable storage en voert die vervolgens uit.
Bij fatsoenlijke instellingen van je workstation wordt dat niet toegestaan, en daar moeten dan uitzonderingen op worden gemaakt voor Webex, wat het systeem als geheel onveiliger maakt. Met name risico voor allerlei ongewenste RAT en ander malware.

Je zal toch wel begrijpen dat er geen executable files van internet gedownload en geïnstalleerd worden. Maar nee, gelijk een oordeel vellen over een zelfverzonnen situatie bij de overheid die totaal niet klopt.

Je kent Webex kennelijk niet!
Dit is een programma wat je wel kunt installeren op een computer, maar als je het dan opstart download het meteen weer extra code en die voert het dan uit.
Dus als je gebruikers helemaal verbiedt om code te downloaden en uit te voeren dan werkt de Webex client niet! (wel de webversie)
Dit is geen zelfverzonnen situatie hoor, dit is gewoon eigen ervaring.

De web versie download ook een plugin voor in je browser, anders werkt het niet.
Overigens zijn ze die web versie aan het uitfasen en als je echt meeting security wil (end2end encryptie) dan werkt de web versie per definitie niet en de Linux versie ook niet overigens.
Rijksvideobellen heeft die optie echter niet by default aan staan.
Daarnaast kun je meetings beperken tot alleen gebruikers die ingelogt zijn en zelfs alleen tot jouw organisatie behoren. Veel succes met een url enumeration.

12-09-2024, 15:50 door [Anoniem](#) [Reageer met quote](#)

Door Anoniem:

Door Anoniem:

Door Anoniem: "De Rijksoverheid heeft aanbevolen veiligheidsinstellingen en werkt veelal niet met de cloudversie, maar met de clientversie van Webex"

Oh maar dat is nog erger, want die download bij opstarten executable files van internet naar user-writable storage en voert die vervolgens uit.
Bij fatsoenlijke instellingen van je workstation wordt dat niet toegestaan, en daar moeten dan uitzonderingen op worden gemaakt voor Webex, wat het systeem als geheel onveiliger maakt. Met name risico voor allerlei ongewenste RAT en ander malware.

Je zal toch wel begrijpen dat er geen executable files van internet gedownload en geïnstalleerd worden. Maar nee, gelijk een oordeel vellen over een zelfverzonnen situatie bij de overheid die totaal niet klopt.

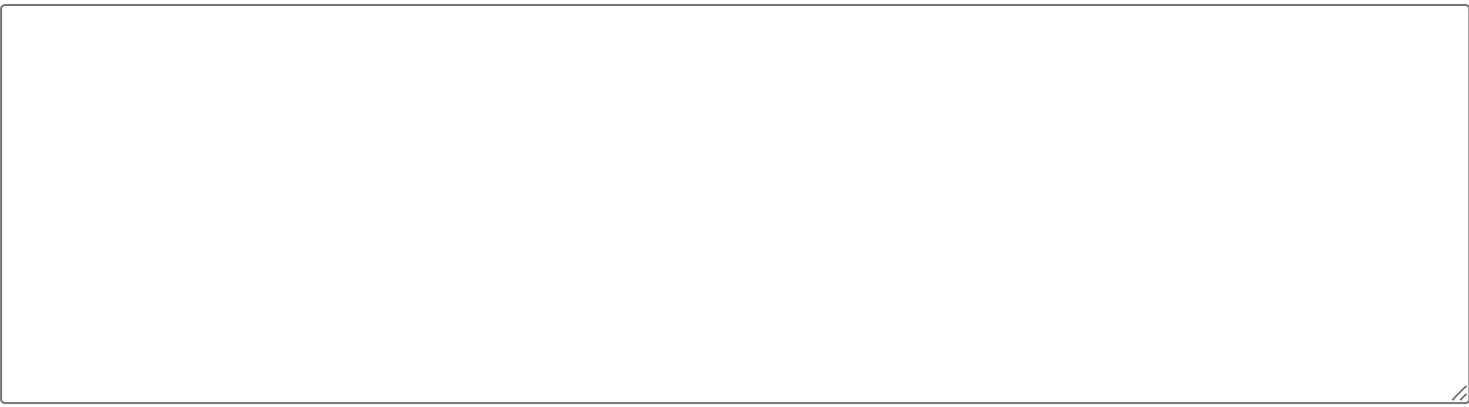
Je kent Webex kennelijk niet!
Dit is een programma wat je wel kunt installeren op een computer, maar als je het dan opstart download het meteen weer extra code en die voert het dan uit.
Dus als je gebruikers helemaal verbiedt om code te downloaden en uit te voeren dan werkt de Webex client niet! (wel de webversie)
Dit is geen zelfverzonnen situatie hoor, dit is gewoon eigen ervaring.

Ik mag dan niet alles over Webex weten, maar mijn ervaring is totaal anders.
Ik heb 4 jaar geleden bij de overheid gewerkt voor een half jaar durend project en gezien dat de laptops waar men mee werkt al voorzien van de software die nodig is.
Webex is al voorgeïnstalleerd, want iedereen gebruikt dat. Dus geen extra code die opgehaald wordt van internet.
Updates worden geregeld via 1 of ander software-management programma.
Toegang internet op basis van whitelist.
Rijksoverheid is groot, dus mogelijk verschillende werkwijzes, beheer e.d.

Reageren

Ondersteunde bbcodes

Je bent niet [ingelogd](#) en reageert "[Anoniem](#)". Dit betekent dat Security.NL geen accountgegevens (e-mailadres en alias) opslaat voor deze reactie. Je reactie wordt niet **direct geplaatst** maar eerst gemodereerd. Als je nog geen account hebt kun je [hier direct een account aanmaken](#). Wanneer je Anoniem reageert moet je **altijd** een captchacode opgeven.



Nieuwe code

Herhaal code:

Preview

Reageren