BEVEILIGING EN PRIVACY VOOR LOGITECH VIDEOSAMENWERKING

INLEIDING

De frequentie en complexiteit van cyberaanvallen nemen wereldwijd toe en brengen aanzienlijke risico's met zich mee voor organisaties met een hybride werkomgeving die met de dag meer verspreid en gevirtualiseerd wordt.

Cybercriminaliteit kan tegenwoordig overal vandaan komen. Hackers maken misbruik van kwetsbaarheden in zowel software als hardware, zoals camera's, headsets en andere apparaten.

In deze whitepaper delen we onze benadering van beveiliging en privacy voor apparaten met CollabOS. Momenteel zijn dit de Rally Bar, Rally Bar Mini, RoomMate, Tap Scheduler en Tap IP.

WAT IS COLLABOS?

CollabOS is het unifying-besturingssysteem dat op geselecteerde Logitech-apparaten voor videosamenwerking wordt uitgevoerd. Dankzij CollabOS kunnen deze apparaten naadloos samenwerken en voortdurend verbeterd worden. Ook zijn ze eenvoudig te implementeren en beheren, waardoor u iedereen hoogwaardige en gelijkwaardige vergaderervaringen kunt bieden.

Daarbij vereenvoudigt CollabOS de implementatie en het beheer van videovergaderen verder door Logitech-hardware en toepassingen en planningsservices van derden te integreren, zoals Microsoft Teams, Zoom en Robin.

CollabOS verbetert continu de gebruikerservaring voor deelnemers aan videovergaderingen en verlengt tegelijkertijd de levensduur van uw VC-investering. Firmware-updates met nieuwe functies, verbeteringen en beveiligingsmaatregelen worden automatisch draadloos en gratis naar uw apparaten verzonden.

APPARATEN MET COLLABOS

- **Rally Bar** en **Rally Bar Mini** zijn de beste alles-in-één videobars van Logitech voor grote, middelgrote en kleine vergaderruimtes, met een unieke optische camera, gelijktijdige tweerichtingsaudio en een secundaire speciale AI-camera. Beiden kunnen met uitzonderlijke flexibiliteit en gemak worden toegepast in USB- of appliance mode.

  Meer informatie over Rally Bar en Rally Bar Mini

- **RoomMate** is een apparaat voor videovergaderen voor ondersteunde conference camera's en randapparatuur, waaronder Rally System, MeetUp en audio van derden. U kunt hiermee eenvoudig Microsoft Teams® Rooms implementeren op Android, Zoom Rooms Appliances en andere toonaangevende services voor videovergaderen.

  Meer informatie over RoomMate

- **Tap IP** is een op het netwerk aangesloten touchcontroller waarmee u eenvoudig deel kunt nemen aan videovergaderingen op verschillende platforms en toepassingen. Met een ruim scherm van 10,1", een laag profiel en een bewegingssensor om altijd gebruiksklaar te zijn, biedt Tap IP mogelijkheden voor het eenvoudig delen van inhoud en een consistente vergaderervaring in alle ruimtes.

  Meer informatie over Tap IP

- **Tap Scheduler** is een speciaal ontworpen planningspaneel voor vergaderruimtes dat de ervaring op kantoor verbetert. Met Tap Scheduler kunt u eenvoudig vergaderdetails bekijken en een ruimte reserveren voor ad hoc of toekomstige vergaderingen, met gekleurde led-lampjes die de beschikbaarheid op afstand laten zien, zodat werknemers snel een beschikbaar plekje kunnen vinden.

  Meer informatie over Tap Scheduler

BEVEILIGING EN PRIVACY

Beveiliging en privacy zijn essentiële aspecten van het ontwerp van alle Logitech VC-producten. CollabOS draait op Android 10, dat eersteklas beveiliging, privacy en prestaties biedt.

Logitech-producten worden ontwikkeld met behulp van een veilige ontwikkelingscyclus die de best practices uit de branche volgt tijdens het ontwerpen, ontwikkelen en in gebruik nemen van producten. We voldoen aan de beveiligingsverwachtingen en overtreffen deze door beveiliging vanaf de vroegste ontwerpfasen in te bouwen.

Hier komt ook een beoordeling van het productontwerp door een Security Review Board bij kijken. Deze bestaat uit beveiligingsexperts uit de hele organisatie. We controleren de beveiliging van systemen en software grondig tijdens de ontwikkeling en het testen. En we volgen STRIDE, de branchenorm voor het classificeren van beveiligingsbedreigingen.

Opmerking: tenzij anderszins aangegeven zijn de beveiligings- en privacyfuncties die in deze whitepaper worden beschreven van toepassing op de vijf hierboven genoemde apparaten. Deze worden in de hele paper aangeduid met 'CollabOS-apparaten'.

INFORMATIEBEVEILIGING

SECURE DEVELOPMENT LIFECYCLE (SDLC)

De poorten voor beveiligingsbeoordeling worden geïmplementeerd in elke fase van de systeemontwikkeling voor de SDLC van Logitech voor CollabOS-apparaten, inclusief ontwerp, implementatie en release. Tijdens de ontwerpfase worden alle ontwerpdocumenten beoordeeld door interne en externe beveiligingsdeskundigen.

Er worden zowel geautomatiseerde als handmatige beoordelingen uitgevoerd van de code die door het ontwikkelteam wordt geproduceerd tijdens de implementatiefase. Statische analyse wordt op alle broncodes uitgevoerd en problemen die naar boven komen worden gemarkeerd en beoordeeld door het ontwikkelteam en beveiligingsspecialisten.

Elke software-ontwikkeling voor CollabOS volgt branchenormen, waaronder (maar niet beperkt tot) de volgende:

- Android Secure Coding Standard
- SEI CERT Oracle Coding Standard voor Java
- SEI CERT C Coding Standard
- SEI CERT C Coding Standard

Voordat software wordt uitgegeven, wordt deze uitgebreid getest op functionaliteit en beveiliging. Systeemupdates en nieuwe versies volgen ook de SDLC. Software op locatie wordt onderhouden en geüpdatet met beveiligingspatches voor problemen die tussen belangrijke versies worden ontdekt.

BEVEILIGING EN PRIVACY DOOR ONTWERP

Beveiliging en privacy zijn in het ontwerp van de CollabOS-apparaten ingebouwd. Vanaf het begin van de productontwikkeling tot de implementatie, release en updates.

Hier volgt een niet-exclusieve lijst van de stappen die we nemen om de beveiliging van deze apparaten te versterken:

- **Een stevige fundering als basis:** ten eerste is het platform gebaseerd op Android 10, dat verbeterde beveiliging en stabiliteit biedt.
- **Universele, standaard wachtwoorden vermijden:** conform de aanbevolen procedures in de branche en de Californische staatswet gebruiken CollabOS-apparaten nooit een algemeen en standaard wachtwoord. De apparaten hebben geen standaard wachtwoord.
- **Software up-to-date houden:** firmware-updates 'via de lucht' worden gebruikt om CollabOS-apparaten voortdurend up-to-date te houden met de nieuwste release.
- **De software-integriteit behouden:** alle software-afbeeldingen worden tijdens de productie digitaal ondertekend en verspreid via beveiligde communicatielinks. CollabOS-apparaten verifiëren de handtekening van elke softwareafbeelding voordat de software wordt geïnstalleerd of geüpgraded. Hierdoor worden de integriteit en authenticiteit behouden.
- **Veilig communiceren:** vanaf versie 1.7 van CollabOS wordt voor alle communicatie tussen CollabOS-apparaten en de cloud TLS (Transport Level Security) versie 1.2 en 1.3 gebruikt. TLS 1.1 en 1.0 zijn uitgeschakeld op CollabOS-apparaten en worden niet meer weergegeven in beveiligingsscans. Toepassingen die op het platform lopen kunnen gelijksoortige of aanvullende vormen van communicatie gebruiken. We raden u aan om bij de serviceprovider van de app te informeren naar hun beveiligingsprotocollen.
- **Persoonlijke gegevens beschermen:** hoewel CollabOS-apparaten geen persoonlijk identificeerbare informatie op het apparaat bevatten of opslaan, kunnen videoserviceproviders persoonlijk identificeerbare informatie (PII) opslaan binnen hun apps. We raden u aan om bij de serviceprovider van de app te informeren naar hun PII-beleid.

INFORMATIEBEVEILIGING

BEVEILIGING VAN DE APPARAATTOEPASSING

CollabOS-apparaten bevatten verschillende toepassingen die dagelijks worden gebruikt. Om het apparaat te beveiligen, moet Logitech de toepassingen die op het apparaat staan zorgvuldig beheren.

Door de toepassing in de whitelist op te nemen, wordt er precies gecontroleerd welke toepassingen gebruikt kunnen worden. Voordat de software wordt verzonden, verwijderen we niet-essentiële apps, services en apparaatdrivers of schakelen we deze uit. Dit maakt deel uit van de beveiliging van de software en vermindert de kwetsbaarheid voor aanvallen. Alle CollabOS-apparaten gebruiken de ingebouwde SELinux Policies, een onderdeel van het Android-systeem.

FUNCTIE VOOR TERUGROLBEVEILIGING

De door CollabOS ondersteunde apparaten hebben een functie die voorkomt dat een geüpdatet systeem teruggezet wordt naar een eerdere en mogelijk minder veilige softwareset.

HARDWAREBEVEILIGING

Alle door CollabOS ondersteunde apparaten zijn uitgerust met verschillende functies die de beveiliging van het apparaat verbeteren. Er wordt een trust enclave gebruikt om vereiste geheimen of sleutels op het apparaat te beschermen. De hardware gebruikt veilig opstarten om de validiteit van opstartsoftware en systeem-firmware te verifiëren die tijdens de productie ondertekend werden.

VALIDATIE VAN BEVEILIGING

Interne processen voor kwaliteitsbewaking gebruiken testsuites voor de beveiliging van software-onderdelen om elke softwareversie te controleren op beveiligingsproblemen. Pas als de software door de testsuitepoort is gekomen, kan de software worden vrijgegeven.

FIREWALL-REGELS: POORTFILTERING/-BLOKKERING

Alle door CollabOS ondersteunde apparaten implementeren hun eigen firewallregels om poortfiltering en -blokkering te bewerkstelligen. Hierdoor wordt het aanvalsoppervlak dat aan het netwerk wordt blootgesteld, verkleind.

EXTERNE APPARAAT-INDICATOREN VOOR OPNAME EN PRIVACY

Alle CollabOS-opnameapparaten, inclusief microfoons en camera's, hebben duidelijke indicatoren die aangeven wanneer ze in gebruik zijn. Rally Bar en Rally Bar Mini worden verzonden met lensdoppen voor de conference camera's.

Opmerking: deze functie is niet van toepassing op Tap IP, Tap Scheduler of RoomMate die geen camera's of microfoons hebben en geen video of geluid kunnen opnemen.

SANDBOXING VAN EEN TOEPASSING

Toepassingen kunnen elkaar niet storen op het platform door ingebouwde sandboxing van de toepassing. Elke toepassing en zijn data hebben hun eigen ruimte waarin ze werken en kunnen niet communiceren of de uitvoering van andere toepassingen storen. Hieronder valt de mogelijkheid om data te lezen en schrijven die in de sandbox van elke toepassing wordt bewaard.

BEVEILIGEN VAN DATA: VERSLEUTELDE OPSLAG

Versleutelde opslag op hardwareniveau wordt gebruikt om alle data op te slaan op door CollabOS ondersteunde apparaten.

GEGEVENSBEVEILIGING VAN BACK-END

Communicatie tussen door CollabOS ondersteunde apparaten en Logitech-backendsystemen die deze apparaten ondersteunen, inclusief draadloze updates, vindt plaats via versleutelde kanalen met behulp van TLS (Transport Layer Security). Dit biedt zowel een versleuteling van gegevens in transit als verificatie van het systeem waarmee het apparaat communiceert.

We maken gebruik van het framework en de infrastructuur van Amazons Internet of Things (IoT) om veilige communicatie tussen het apparaat en de backend mogelijk te maken en data-at-rest te beveiligen in de cloud.

KWETSBAARHEID EN RISICOBEHEER

We monitoren actief de beveiliging van onze producten en leveren tijdige updates om alle bekende kwetsbaarheden aan te pakken.

REACTIE OP INCIDENTEN

Logitech nodigt klanten en beveiligingsonderzoekers uit om problemen te melden die zich met onze producten voordoen, zodat ze op locatie opgelost kunnen worden. We nemen deel aan een openbaar bug bounty-programma waarmee onderzoekers kunnen helpen de beveiliging van onze producten te verbeteren door problemen te melden die ze vinden en erkenning krijgen voor hun ontdekkingen. Logitech geeft passende erkenning aan verantwoordelijke melders van beveiligingsincidenten die gegrond en uitvoerbaar zijn bevonden.

Bovendien worden incidenten geregistreerd en zo snel mogelijk behandeld. We verwachten van degenen die incidenten melden dat ze aanvaarde praktijken volgen voor verantwoorde openbaarmaking.

AANVULLENDE HULPBRONNEN

Ga naar logitech.com/vc voor meer informatie over apparaten die door CollabOS worden ondersteund, waaronder Rally Bar, Rally Bar Mini, RoomMate, Tap IP en Tap Scheduler.

CONTACT

Ga naar logitech.com/security als u een beveiligingskwestie voor Logitech-producten wilt melden. Ga naar logitech.com/nl-nl/contact voor andere vragen.

Logitech Inc.
7700 Gateway Blvd.
Newark, CA 94560
Gepubliceerd in november 2023