BEVEILIGING EN PRIVACY VAN LOGITECH-APPARATEN VOOR VIDEO COLLABORATION

RALLY BAR, RALLY BAR MINI EN ROOMMATE

INLEIDING

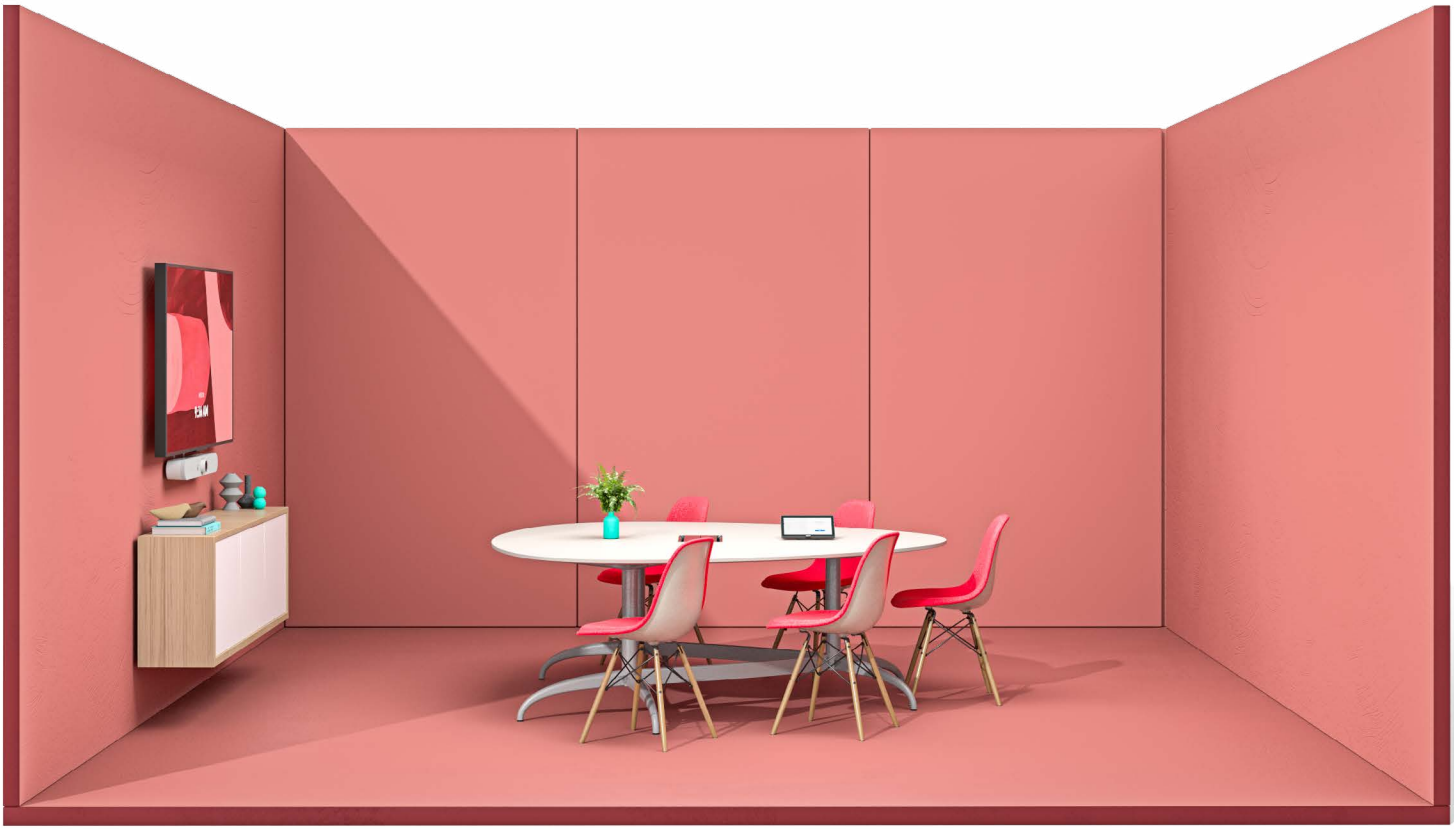
Deze whitepaper beschrijft benadering van beveiliging en privacy voor Logitech® Rally Bar, Logitech Rally Bar Mini en Logitech RoomMate.

Logitech, een wereldleider in producten die mensen verbinden aan de digitale ervaringen waar ze om geven, biedt een assortiment van collaborationtools die gemakkelijk te gebruiken zijn met vrijwel alle video conferencing applicaties.

Rally Bar en Rally Bar mini zijn Loigtech's beste alles-in-één videobars voor middelgrote en kleine vergaderruimtes. Met fantastisch beeld, krachtige audio en AI-gestuurde prestaties, zetten deze vergadercamera's een nieuwe standaard voor video collaboration. Beide kunnen met uitzonderlijke flexibiliteit en gemak op schaal worden toegepast in USB- of appliance mode.

Bij Rally Bar, Rally Bar Mini en RoomMate zijn beveiliging en privacy essentiële aspecten van het productontwerp. Ze zijn elk gebaseerd op Android 10, dat een eersteklas beveiliging, privacy en prestaties levert. In deze gebieden is Android 10 een aanzienlijke verbetering op vorige versies van het Android-besturingssysteem.

Deze Logitech-producten zijn ontwikkeld met behulp van een veilige ontwikkelingscyclus die de best practices van de branche volgt tijdens het ontwerp, de ontwikkeling en de uitvoering van het product. We voldoen aan de beveiligingsverwachtingen of overtreffen deze zelfs door vanaf de vroegste ontwerpstadia beveiliging in te bouwen. Dit omvat een beoordeling van het productontwerp door een beoordelingscomité voor beveiliging, welke is samengesteld 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 op, de branchenorm voor het classificeren van beveiligingsbedreigingen.



INFORMATIEBEVEILIGING

SECURE DEVELOPMENT LIFECYCLE (SDLC)

Rally Bar, Rally Bar Mini en RoomMate werden ontwikkeld volgens de aanbevolen procedures voor een veilige ontwikkelingscyclus. De SDLC beoordeeld de beveiliging in elk stadium van de systeemontwikkeling: ontwerp, implementatie en release. Tijdens de ontwerpfase worden alle ontwerpdocumenten beoordeeld door interne en externe beveiligingsdeskundigen.

Er worden tijdens de implementatiefase zowel geautomatiseerde als handmatige beoordelingen uitgevoerd van de code die door het ontwikkelteam wordt geproduceerd. 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 Rally Bar, Rally Bar Mini en RoomMate 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 Rally Bar, Rally Bar Mini en RoomMate 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:

- **Beginnen met een stevige fundering:** Ten eerste is het platform gebaseerd op Android 10, dat verbeterde beveiliging en stabiliteit biedt.
- **Algemene en standaard wachtwoorden vermijden:** Volgens de aanbevolen procedures in de branche en de Californische staatswet gebruiken Rally Bar, Rally Bar Mini en RoomMate nooit een algemeen en standaard wachtwoord. De apparaten hebben geen standaard wachtwoord.
- **Houd de software geüpdatet:** 'Over the air'-software-updates houden de software voor Rally Bar, Rally Bar Mini en RoomMate voortdurend actueel met de nieuwste versie.
- **De software-integriteit behouden:** Alle software-afbeeldingen zijn versleuteld en digitaal ondertekend tijdens de productie. Rally Bar, Rally Bar Mini en RoomMate verifiëren de handtekening van elke softwareafbeelding voordat de software wordt geïnstalleerd of geüpgraded. Hierdoor worden de integriteit en authenticiteit behouden.
- **Veilig communiceren:** Alle communicatie tussen Rally Bar/Rally Bar Mini/RoomMate en de cloud worden uitgevoerd met Transport Level Security (TLS). 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 Rally Bar, Rally Bar Mini en RoomMate 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

Rally Bar, Rally Bar Mini en RoomMate bevatten enkele toepassingen die bij het dagelijkse gebruik 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 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. Rally Bar en Rally Bar Mini gebruiken de ingebouwde SELinux Policies, een onderdeel van het Android-systeem.

BEVEILIGING VAN DE HARDWARE

De hardware-onderdelen van de Rally Bar, Rally Bar Mini en RoomMate zijn uitgerust met speciale 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. Een op de hardware gebaseerde anti-rollbackfunctie is ingeschakeld om te voorkomen dat een geüpdatet systeem teruggezet wordt naar een eerdere, en mogelijk minder veilige softwareset.

Fysieke beveiliging wordt verder verbeterd met manipulatievrije en -bestendige afdekkingen voor de hardwarepoorten.

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

Rally Bar, Rally Bar Mini en RoomMate 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 opnameapparaten die onderdeel zijn van Rally Bar, Rally Bar Mini en RoomMate, waaronder microfoons en camera's, hebben duidelijke indicatoren als ze in gebruik zijn. Rally Bar en Rally Bar Mini worden verzonden met lensdoppen voor de vergadercamera's.

SANDBOXING VAN EEN TOEPASSING

Toepassingen kunnen elkaar niet storen op het platform door gebruik van 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 Rally Bar, Rally Bar Mini en RoomMate.

GEGEVENSBEVEILIGING VAN BACK-END

De communicatie tussen Rally Bar/Rally Bar Mini/ RoomMate en de back-endsystemen van Logitech die hen ondersteunen, waaronder 'over de air'-updates, wordt via versleutelde kanalen uitgevoerd en maakt gebruik van Transport Layer Security (TLS). TLS biedt zowel versleuteling van de data-in-transit als authenticatie 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 back-end 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

Voor meer informatie over Rally Bar, Rally Bar Mini en RoomMate, ga naar onze website op logitech.com/vc.

CONTACT

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

Ga naar logitech.com/contact voor andere vragen.

Logitech Inc.
7700 Gateway Blvd.
Newark, CA 94560
Gepubliceerd in november 2020