

logitech®

SEGURANÇA E PRIVACIDADE NOS DISPOSITIVOS DE VIDEOCOLABORAÇÃO DA LOGITECH

RALLY BAR, RALLY BAR MINI E ROOMMATE



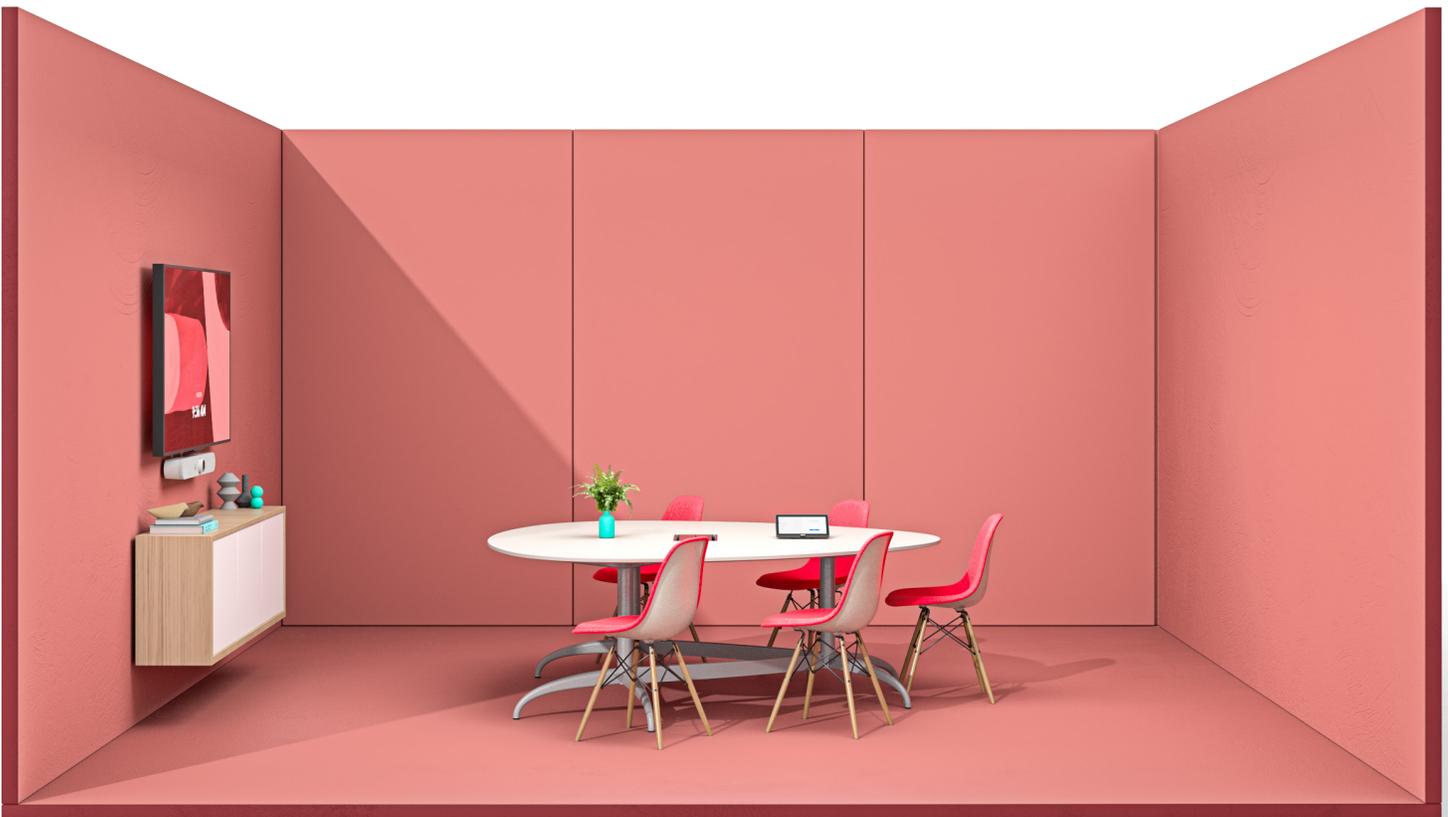
O artigo técnico a seguir descreve nossa abordagem à segurança e privacidade na Logitech® Rally Bar, Logitech Rally Bar Mini e Logitech RoomMate.

Como líder mundial em produtos que conectam pessoas às experiências digitais com as quais elas se preocupam, a Logitech oferece uma variedade de ferramentas de colaboração que são fáceis de usar com praticamente qualquer aplicativo em quase todos os lugares.

A Rally Bar e a Rally Bar Mini são as principais barras de vídeo multifuncionais da Logitech para salas de reunião pequenas e médias. Com lentes brilhantes, áudio potente e desempenho orientado por IA, essas câmeras de conferência definem um novo padrão para a videoconferência. Ambas podem ser implantadas em escala usando o modo appliance ou USB, com extrema flexibilidade e facilidade.

A segurança e a privacidade são aspectos essenciais do design da Rally Bar, Rally Bar Mini e RoomMate. Todos os três produtos são baseados no Android 10, que fornece a melhor segurança, privacidade e desempenho. Nessas áreas, o Android 10 é uma melhoria significativa em relação a versões anteriores desse sistema operacional.

Esses produtos da Logitech foram desenvolvidos com um ciclo de vida de desenvolvimento seguro, conforme as práticas recomendadas da indústria, durante o design, desenvolvimento e lançamento. Para atendermos ou superarmos as expectativas quanto à segurança, ela é incorporada desde os primeiros estágios de design. Isso inclui uma avaliação do design do produto, realizada por um conselho composto de especialistas em segurança provenientes de toda a organização. Verificamos a segurança nos sistemas e software durante o desenvolvimento e os testes com todo o rigor. Além disso, seguimos o padrão [STRIDE](#) da indústria para classificar ameaças à segurança.



CICLO DE VIDA DE DESENVOLVIMENTO SEGURO (SDL, NA SIGLA EM INGLÊS)

A Rally Bar, Rally Bar Mini e RoomMate foram desenvolvidas segundo as práticas recomendadas para um ciclo de vida de desenvolvimento seguro. O SDL tem avaliações de segurança em cada estágio do desenvolvimento de sistemas: design, implementação e lançamento. Durante o estágio de design, todos os documentos são avaliados por especialistas em segurança de dentro e fora da empresa.

O estágio de implementação conta com avaliações tanto manuais quanto automatizadas do código produzido pela equipe de desenvolvimento. A análise estatística é realizada em todos os códigos-fonte, e quaisquer problemas resultantes são sinalizados e avaliados pela equipe de desenvolvimento e pelos especialistas em segurança.

Todo o desenvolvimento de software da Rally Bar, Rally Bar Mini e RoomMate segue os padrões da indústria, incluindo, entre outros, os seguintes:

- # [Android Secure Coding Standard](#)
- # [SEI CERT Oracle Coding Standard for Java](#)
- # [SEI CERT C Coding Standard](#)
- # [SEI CERT C++ Coding Standard](#)

Antes de um software ser lançado, ele passa por uma série completa de testes de funcionalidade e segurança. Atualizações e lançamentos de software também seguem o SDL. Os softwares que já estão no mercado são mantidos e atualizados com quaisquer patches de segurança necessários no caso de problemas detectados entre os principais lançamentos.



SEGURANÇA E PRIVACIDADE POR DESIGN

A Rally Bar, Rally Bar Mini e RoomMate incluem segurança e privacidade em seu design, desde o início do desenvolvimento do produto até a implementação, lançamento e atualizações.

A seguir, confira uma lista breve com as etapas que realizamos para fortalecer a segurança desses dispositivos:

- # **Começar com uma base sólida:** por padrão, a plataforma é baseada no Android 10, que inclui segurança e estabilidade aprimoradas.
- # **Evitar senhas padrão universais:** a Rally Bar, Rally Bar Mini e RoomMate seguem as práticas recomendadas da indústria e a legislação da Califórnia no que diz respeito a nunca usar uma senha padrão universal. Os dispositivos não têm uma senha padrão.
- # **Manter o software atualizado:** as atualizações de software sem fio são usadas para mantê-lo sempre atualizado com a versão mais recente na Rally Bar, Rally Bar Mini e RoomMate.
- # **Manter a integridade do software:** todas as imagens do software são criptografadas e assinadas digitalmente durante a produção. A Rally Bar, Rally Bar Mini e RoomMate confirmam a assinatura de cada imagem de software antes da instalação ou upgrade. Dessa forma, mantemos a integridade e a autenticidade.
- # **Comunicar com segurança:** todas as comunicações entre a Rally Bar/Rally Bar Mini/RoomMate e a nuvem usam Protocolo TLS. Os aplicativos em execução na plataforma talvez usem formas semelhantes ou adicionais de comunicação. Recomendamos confirmar com os provedores de serviço dos aplicativos os protocolos de segurança usados.
- # **Proteger dados pessoais:** apesar de a Rally Bar, Rally Bar Mini e RoomMate não conterem ou armazenarem informações de identificação pessoal (PII, na sigla em inglês) no dispositivo, os provedores de serviço de vídeo talvez armazenem esses dados em seus respectivos aplicativos. Recomendamos confirmar com os provedores de serviço a política de PII usada.

SEGURANÇA DOS APLICATIVOS NO DISPOSITIVO

A Rally Bar, Rally Bar Mini e RoomMate contêm diversos aplicativos usados em operações de rotina. Para proteger o dispositivo, a Logitech precisa gerenciar com cuidado os aplicativos presentes nele.

Durante o processo de autorização de aplicativos, podemos controlar exatamente quais deles são permitidos. Como parte da proteção do software antes do envio, também removemos ou desativamos os aplicativos, serviços e drivers não essenciais para reduzir a superfície de ataque. Tanto a Rally Bar quanto a Rally Bar Mini usam as políticas SELinux integradas, um componente do sistema Android.

SEGURANÇA DO HARDWARE

Os componentes de hardware da Rally Bar, Rally Bar Mini e RoomMate são equipados com diversos recursos que aprimoram a segurança do dispositivo. Um enclave de confiança é usado para proteger quaisquer segredos ou chaves exigidos, no dispositivo. O hardware utiliza a inicialização segura para confirmar a validade do software de inicialização e o firmware do sistema, que foram assinados durante a produção. Um recurso antirreversão com base em hardware é ativado para impedir que um sistema atualizado retorne para uma versão de software anterior e provavelmente menos segura.

A segurança física é ainda mais aprimorada com as tampas resistentes antiviolação nas portas do hardware.

VALIDAÇÃO DA SEGURANÇA

Os processos de garantia de qualidade internos utilizam uma série de testes de segurança nos componentes do software para verificar se há vulnerabilidades na segurança do software a ser lançado. O software não poderá ser lançado até que ele passe nesses testes.

REGRAS DE FIREWALL: BLOQUEIO/FILTRAGEM DE PORTA

A Rally Bar, Rally Bar Mini e RoomMate implementam as próprias regras de firewall para realizar o bloqueio e a filtragem de porta. Assim, reduzimos a superfície de ataque exposta à rede.

INDICADORES DE DISPOSITIVOS EXTERNOS PARA GRAVAÇÃO E PRIVACIDADE

Todos os dispositivos de gravação que compõem a Rally Bar, Rally Bar Mini e RoomMate, incluindo microfones e câmeras, têm indicadores claros quando estão em uso. Tanto a Rally Bar quanto a Rally Bar Mini são enviadas com tampas nas lentes das câmeras de conferência.

ÁREA RESTRITA PARA APLICATIVOS

Os aplicativos não podem interferir uns nos outros na plataforma graças ao uso da área restrita para aplicativos integrada. Cada aplicativo e seus respectivos dados recebem o próprio espaço para trabalhar e não podem comunicar-se ou interferir na execução de outros aplicativos. Essa restrição abrange a leitura e gravação de dados, que é mantida na área de restrição de cada aplicativo.

PROTEÇÃO DE DADOS: ARMAZENAMENTO CRIPTOGRAFADO

O armazenamento criptografado no nível do hardware é usado pela Rally Bar, Rally Bar Mini e RoomMate para manter todos os dados no dispositivo.

SEGURANÇA DE DADOS COM BACK-END

A comunicação entre a Rally Bar/Rally Bar Mini/RoomMate e os sistemas de back-end da Logitech que oferecem suporte a elas, incluindo atualizações sem fio, ocorre em canais criptografados usando TLS. Esse protocolo fornece tanto criptografia de dados em movimento quanto autenticação do sistema com o qual o dispositivo está se comunicando.

Aproveitamos o framework e a infraestrutura da Internet das coisas (IoT, na sigla em inglês) da Amazon para permitir a comunicação entre o dispositivo e o back-end, além de proteger os dados em repouso na nuvem.



Ativamente monitoramos a segurança dos nossos produtos e fornecemos atualizações oportunas para corrigir quaisquer vulnerabilidades conhecidas.

RESPOSTA A INCIDENTES

A Logitech convida os clientes e os analistas de segurança a denunciar problemas encontrados em nossos produtos para que possam ser corrigidos nos produtos que estão no mercado. Participamos de um programa de recompensa por bugs, no qual analistas podem ajudar a aprimorar a segurança dos nossos produtos ao reportar problemas encontrados e receber o crédito por sua descoberta. A Logitech dá o devido crédito aos responsáveis por delatar incidentes de segurança que sejam válidos e acionáveis.

Além disso, os incidentes são gravados e respondidos assim que possível. Esperamos que essas denúncias de incidentes sigam práticas aceitas para uma divulgação responsável.

RECURSOS ADICIONAIS

Para saber mais sobre a Rally Bar, Rally Bar Mini e RoomMate, acesse o nosso site em logitech.com/vc.

CONTATO

Para denunciar uma suspeita relacionada à segurança nos produtos da Logitech, acesse logitech.com/security.

Para outros assuntos, acesse logitech.com/contact.

