

logitech®

罗技视频协作设备的安全性和隐私性

CC5500E、CC4500E 和 ROOMMATE



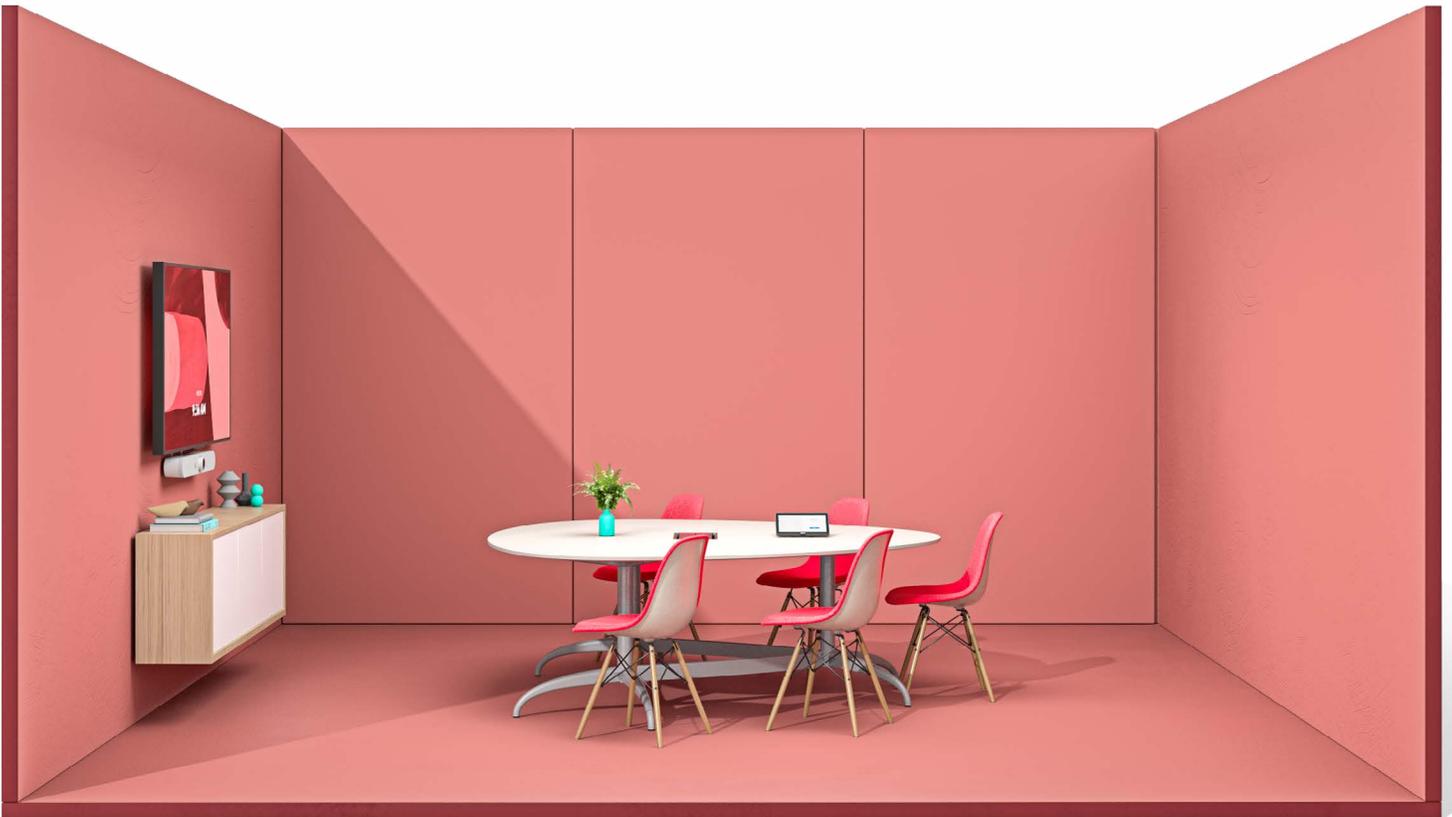
以下白皮书介绍了我们确保罗技® CC5500e、罗技 CC4500e 和罗技 RoomMate 安全性和隐私性的方法。

罗技提供全球领先的产品，为用户架起通往数字体验的桥梁，此外还提供一系列易于使用的协作工具，兼容几乎所有视频会议应用程序，让用户可以随时随地轻松开展协作。

CC5500e 和 CC4500e 是罗技专为中小型会议室设计的卓越一体式视频会议系统。这些会议摄像头具有清晰的画质、出色的音质和由 AI 支持的卓越性能，为视频协作树立了全新标准。两款产品均可在 USB 或设备模式下进行大规模部署，具备出色的灵活性和易用性。

安全性和隐私性是 CC5500e、CC4500e 和 RoomMate 产品设计重点。它们都基于具有出色安全性、隐私性和性能的 Android 10。相较于之前的 Android 操作系统版本，Android 10 在这些方面有了显著的改进。

罗技使用安全开发生命周期开发这些产品，在产品的设计、开发和现场部署期间遵循行业最佳实践。我们在软件设计之初就考虑了安全性，从而达到甚至超过安全预期。这包括由整个组织中的安全专家所组成的安全审查委员会来审查产品设计。在开发和测试过程中，我们严格验证系统和软件的安全性。此外，我们遵循 [STRIDE](#) 行业标准对安全威胁进行分类。



安全开发生命周期 (SDLC)

CC5500e、CC4500e 和 RoomMate 遵循安全开发生命周期的最佳实践进行开发。SDLC 在系统开发的每个阶段（设计、实施和发布）都设有安全审查关卡。在设计阶段，所有设计文档都经过内部和外部安全专家的审查。

在实施阶段，对开发团队编写的代码进行自动化和人工审查。我们会对所有源代码执行静态分析，并标记发现的问题，以供开发团队和安全专家审查。

CC5500e、CC4500e 和 RoomMate 的所有软件开发均遵循行业标准，包括但不限于：

- ✓ [Android Secure Coding Standard \(Android 安全编码标准\)](#)
- ✓ [SEI CERT Oracle Coding Standard for Java \(SEI CERT Oracle Java 安全编码标准\)](#)
- ✓ [SEI CERT C Coding Standard \(SEI CERT C 编码标准\)](#)
- ✓ [SEI CERT C++ Coding Standard \(SEI CERT C++ 编码标准\)](#)

在软件发布之前，它要经过一系列全面的功能和安全测试。系统更新和新版本同样遵循 SDLC，而现场部署的软件则通过安装必要的安全补丁进行维护和更新，以解决在各主要版本之间发现的问题。

设计成就安全性和隐私性

CC5500e、CC4500e 和 RoomMate 自产品开发之始到实施、发布和更新的整个过程中均将安全性与隐私性作为设计要点。

以下列出了我们为增强设备安全性而执行的一部分步骤：

- ✓ **从坚实的基础开始：**作为基准，平台基于具有增强的安全性和稳定性的 Android 10。
- ✓ **避免通用默认密码：**CC5500e、CC4500e 和 RoomMate 遵循行业最佳实践和加利福尼亚州法律规定，从不使用通用默认密码。这些设备没有默认密码。
- ✓ **确保软件更新为新版本：**CC5500e、CC4500e 和 RoomMate 采用在线软件更新方法确保软件始终更新为最新版本。
- ✓ **维护软件的完整性：**在制作过程中，所有软件映像都经过加密和数字签名。在安装或升级软件之前，CC5500e、CC4500e 和 RoomMate 会验证每个软件映像的签名，从而维护其完整性和真实性。
- ✓ **安全通信：**CC5500e/CC4500e/RoomMate 与云之间的所有通信都使用传输层安全协议 (TLS) 执行。在该平台上运行的应用程序可能会采用类似或其他形式的通信。我们建议您向应用程序服务提供商咨询他们的安全协议。
- ✓ **保护个人数据：**尽管 CC5500e、CC4500e 和 RoomMate 不在设备上包含或存储个人身份信息，但视频服务提供商可能会在其应用程序中存储个人身份信息 (PII)。我们建议您向服务提供商咨询他们的 PII 政策。



设备应用程序安全性

CC5500e、CC4500e 和 RoomMate 包含日常操作中常用的数款应用程序。为确保设备安全，罗技需要妥善管理驻留在设备上的应用程序。

通过将应用程序列入白名单，我们可以准确控制允许使用的应用程序。在发送软件之前，作为保护软件安全的一项利器，我们还删除或禁用了非必要的应用程序、服务和设备驱动程序，从而减少了攻击面。CC5500e 和 CC4500e 利用内置的 SELinux 策略，它是 Android 系统的一个组件。

硬件安全性

CC5500e、CC4500e 和 RoomMate 的硬件组件都具有多项用于增强设备安全性的功能。通过可信安全容器来保护设备上的任何所需的秘密或密钥。硬件利用安全启动来验证在制作过程中签名的启动软件和系统固件的有效性。采用基于硬件的反回滚功能，防止更新后的系统恢复到较早的且可能不太安全的软件集。

硬件端口的防篡改和防覆盖功能进一步增强了物理安全性。

安全验证

内部质量保证流程利用软件组件安全测试套件检查每个软件版本的安全漏洞。如果软件没有通过测试套件中的检查，则不能发布。

防火墙规则 - 端口筛选/阻止

CC5500e、CC4500e 和 RoomMate 实施各自的防火墙规则来实现端口筛选和阻止，从而减少暴露于网络的攻击面。

通过外部设备指示灯指示录制并确保隐私性

CC5500e、CC4500e 和 RoomMate 包含的所有录制设备（包括麦克风和摄像头）在使用时都会亮起明亮的指示灯。CC5500e 和 CC4500e 还为会议摄像头随附了镜头盖。

应用程序沙盒

通过使用内置的应用程序沙盒，可防止平台上的应用程序相互干扰。每个应用程序及其数据都有各自的工作空间，且受到限制，无法与其他应用程序通信或干扰其执行，包括限制对按应用程序沙盒保存的数据进行读取和写入的能力。

保护数据安全 - 加密存储

使用硬件级加密存储来存储 CC5500e、CC4500e 和 RoomMate 上的所有数据。

后端数据安全

CC5500e/CC4500e/RoomMate 与支持它们的罗技后端系统之间的通信（包括在线更新）通过使用传输层安全 (TLS) 协议的加密通道进行通信，该协议可加密传输中的数据，并对设备与之通信的系统进行身份验证。

我们利用亚马逊的物联网 (IoT) 框架和基础设施，来实现设备与后端之间的安全通信，并确保云中静态数据的安全。



我们积极监控罗技产品的安全，并及时提供更新以解决任何已知的漏洞问题。

事件响应

罗技欢迎客户和安全研究人员报告在我们产品中发现的问题，以便就地予以解决。我们参与了一项公共漏洞奖励计划，通过该计划，研究人员可以报告他们发现的问题并获得相应的积分，从而帮助提高罗技产品的安全性。如果发现的安全事件是有效且可操作的，罗技会给予报告者相应的积分。

此外，我们会尽快记录并响应事件，并希望事件报告者遵循已接受的做法报告事件，实现负责的披露。

其他资源

如需了解关于 CC5500e、CC4500e 和 RoomMate 的更多信息，请访问我们的网站：logitech.com/vc。

联系方式

如需报告关于罗技产品安全的问题，请访问 logitech.com/security。

如需咨询其他事宜，请访问 logitech.com/contact。



Logitech Inc.
7700 Gateway Blvd.
Newark, CA 94560
2020 年 11 月发布

本白皮书仅供参考。罗技对本白皮书中提供的信息不作任何明示、暗示或法定的保证。本白皮书按“原样”提供，罗技可能会不时进行更新。

版权所有 © 2020 Logitech。罗技、Logi、Logitech 和罗技标志为罗技欧洲公司和/或其美国及其他国家/地区附属公司的商标或注册商标。所有其他商标均是各自所有者的财产。罗技对于本出版物中可能出现的任何错误不承担任何责任。本白皮书中包含的信息如有更改，恕不事先通知。