illumina®

我们在医疗健康系统中发挥的作用

因美纳对于近期本地运行管理软件（LRM）网络安全隐患的回应

背景信息

在因美纳，我们为全球构建一个完善的医疗健康系统提供支撑，这种系统可以通过基因组数据和健康数据的分享，加速创新，从而为患者提供前沿的诊疗方案。对此，我们深感自豪。

随着数字化基因组学发展的方兴未艾，网络安全隐患已成为领域内各相关方面临的风险之一。

因美纳致力于促进构建医疗健康生态系统，并采取实际行动。我们深知，必须切实解决网络安全隐患，以降低网络风险，谨防数据丢失。

此函旨在阐述因美纳为其测序仪上的本地运行管理软件 Local Run Manager（LRM）所存在的网络安全隐患提供的解决方案。自2022年5月3日起，我们已与客户就该隐患进行了沟通。

正如我们与客户始终同心携手，不断提高安全性，此函也强调了我们针对安全性问题向客户建议的优选应对方案。

情况概述

因美纳已开发并提供了一个短期软件补丁，以防止本地运行管理软件 Local Run Manager（LRM）受到远程代码执行（RCE）的影响。我们已于2022年5月3日起与客户沟通了相关事宜，并将这一问题向全球范围内的监管机构进行了通报。

本地运行管理软件 Local Run Manager（LRM）是以下测序仪默认配置的一部分：NextSeq™ 550Dx、MiSeq™ Dx、NextSeq™ 500/550、MiSeq™、iSeq™ 以及 MiniSeq™ 。作为测序仪上的一种软件应用，LRM亦可被安装于客户自己的硬件设备。

此次网络安全隐患涉及未经身份验证的远程代码执行（RCE）。未经授权的用户或可绕过安全控制，以管理员身份对系统进行不当访问，这可能会影响测序仪的设置、配置、软件、测序仪上的数据或者客户网络。

修复措施

因美纳已开发了一个软件补丁以防止该隐患被远程利用。与此同时，我们正积极开发一个永久性的软件修复方案，旨在为当前及将来的测序仪全面消除这一隐患，一经完成将及时通知客户。

其他安全建议

安全性的多层次保障对于仅供科研用途（RUO）的测序仪与临床获批诊断设备的安全部署至关重要。因美纳强烈建议将测序仪和设备部署于最小的分支网络或安全环境，并通过可信任的设备进行运行；此外，使用防火墙及其他网络策略，以限制入站访问和出站

访问。

未来规划

我们正为用户立即安装针对该隐患的软件补丁提供支持，并且当长期解决方案一经可用时，我们将及时推进实施。因美纳将继续评估并优化我们的系统以确保网络安全，助力在医疗健康领域的持续创新。

在这个医疗健康系统中，所有相关方对于网络安全性抱持主动且警觉的态度至关重要，包括采取优选方案并且针对已识别的隐患采取短期和长期的应对方案。

我们坚信，基因组数据将大幅助益医疗创新及其影响力，涵盖从基础研究到疫苗研发等各个层面。我们期待，与客户保持紧密合作，共同将医疗健康生态系统的效益落到实处，以基因的力量，改善人类健康。