LRM 软件补丁 1.0

illumina®

说明指南

简介

Illumina® 注意到 Local Run Manager 软件存在安全漏洞，并提供了软件补丁来防止他人远程利用此漏洞。

Local Run Manager 是一款独立的软件应用程序，隶属于以下系统的默认配置：

- MiSeq
- MiSeqDx*
- NextSeq 500
- NextSeq 550
- NextSeq 550Dx*
- MiniSeq
- iSeq

*供体外诊断使用。

本指南适用于上面列出的 Illumina 仪器，以及安装了独立版 Local Run Manager 的非仪器计算机。

该漏洞属于未经身份验证的远程命令执行 (RCE)，未经缓解的 CVSS 评分为 10.0 高风险 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)。

上面列出的仪器需要执行以下缓解步骤，以防止未经授权的用户访问一台或多台仪器并执行远程访问攻击。

如果安装程序因为某些原因无法运行，请参见本文档结尾的其他缓解措施部分，或联系 techsupport@illumina.com 寻求更多协助。

请参见获取 Local Run Manager 更新，了解可以通过哪几种方式下载或请求此补丁的副本。

- **v1.0.0 补丁** — 将更新 Local Run Manager Web 配置并禁用远程 Internet Information Services (IIS) 访问。

获取 Local Run Manager 安全补丁

获取 Local Run Manager 安全补丁的方式有四 (4) 种。

选项 1 — 直接下载到您的仪器

获取 Local Run Manager 安全更新的最快方式是直接从托管网站将其下载到仪器。

1. 通过安全电子邮件提供的链接，将补丁安装程序下载到您的仪器。
2. 将文件传输到仪器上的 C:\Illumina 文件夹。
3. 按照*应用 Local Run Manager 安全补丁（第 3 页）*中的说明操作。

选项 2 — 将补丁安装程序下载到计算机，并通过 U 盘/共享文件夹传输到仪器

如果无法将补丁安装程序下载到仪器，建议将其下载到单独的计算机，然后再传输到仪器。

使用 U 盘之前，请向您的安全代表确认该驱动器的完整性。（建议）

1. 通过安全电子邮件提供的链接将补丁安装程序下载到您的计算机或笔记本电脑。
2. 将下载的补丁安装程序从计算机复制到 U 盘或共享文件夹。
3. 如果使用 USB 驱动器，则将其插入仪器。
4. 将 U 盘或共享文件夹中的补丁安装程序复制到仪器上的 C:\Illumina 文件夹。
5. 按照*应用 Local Run Manager 安全补丁（第 3 页）*中的说明操作。

选项 3 — 请求技术支持

Illumina 技术支持代表将使用以下方法之一引导您完成修补过程：

- 技术支持远程登录
  技术支持代表将远程访问分析仪并代表客户安装补丁。

  系统必须允许远程访问。如果有任何疑问，请向您当地的 IT 代表请求协助。

- 引导说明
  技术支持代表将通过电话提供引导说明。请联系您当地的技术支持代表以寻求协助。

选项 4 — 向 Illumina 订购预先配置的驱动器

客户可以免费订购受写保护的 U 盘。要订购已安装补丁的驱动器，请联系 techsupport@illumina.com。

可能会因为运输延迟或库存不足而影响送货时间。为了尽快保护系统，强烈建议使用能够提供最有效解决途径的方法来实施保护。

应用 Local Run Manager 安全补丁 v.1.0 安装程序

执行 Illumina MSI (Microsoft Installer) 将更新 Local Run Manager Web 服务器配置，以防止执行任何用户上传的内容，并阻止通过 LAN 网络连接对 Local Run Manager Web 界面的所有远程访问。

对于使用 Local Run Manager Web 界面来远程访问仪器的用户，安装此补丁后，该工作流程将停止执行。Illumina 计划日后推出针对此问题的永久性软件修补程序，来恢复此功能。如果因此而导致已建立的工作流程中断，请联系 techsupport@illumina.com 寻求进一步的协助。

MSI 安装程序适用于所有版本的 Local Run Manager，并将根据仪器/计算机上安装的 Local Run Manager 版本自动确定正确的修补程序。

此 MSI 安装程序还将创建审核文件，显示此缓解措施已实施并含时间戳，以反映其已正确安装。

运行 MSI 安装程序 – MSI 安装程序首次运行时将修补系统并创建含完成时间的审核文件。

再次运行 MSI 安装程序将显示 Repair（修复）选项，用户可以选择重新应用或回滚补丁。注意：回滚该补丁将导致仪器配置不安全。

应用 Local Run Manager 安全补丁

要安装补丁，请执行以下操作：

1. 使用管理员帐户（如 sbsadmin）登录系统。

   Illumina 建议在仪器未运行时应用补丁。如果仪器正在执行某项运行，补丁会在运行完成后立即应用。

2. 找到已下载到系统的补丁。
3. 将补丁安装程序移动到 C:\Illumina 文件夹（不受软件限制策略约束）。
4. 双击安装程序图标以启动界面。
5. 应用程序加载后，选择Next（下一步）开始安装补丁。
6. 在“Installation Completion（安装完成）”屏幕中选择 Finish（完成）。

如果需要验证安装报告，请参见*验证*（第 4 页）。

安装结束后需要重新启动。

修复

如果出现错误，客户可以按以下说明执行安装修复：

1. 使用管理员帐户（如 sbsadmin）登录系统。
2. 找到已下载到系统的补丁。
3. 将补丁安装程序移动到 C:\Illumina 文件夹（不受软件限制策略约束）。
4. 双击安装程序图标以启动界面。
5. 安装程序将自动检测配置工具之前是否已执行并提供新选项：
   a. 更改：灰显且不可用
   b. 修复：修复错误并提供重新配置选项。
   c. 删除：卸载补丁并将其恢复为默认配置（请参见*卸载*（第 3 页））
6. 在“Installation Completion（安装完成）”屏幕中选择 Finish（完成）。

如果需要验证安装报告，请参见*验证*（第 4 页）。

安装结束后需要重新启动。

卸载

卸载补丁会撤销对应用程序主机配置文件所做的修改。

1. 使用管理员帐户（如 sbsadmin）登录系统。
2. 找到已下载到系统的补丁。

3. 将补丁安装程序移动到 C:\Illumina 文件夹（不受软件限制策略约束）。
4. 双击安装程序图标以启动界面。
5. 选择 Remove（删除）以卸载补丁并将所有值恢复为默认设置。
6. 选择 Remove（删除）以确认选择卸载补丁并将所有值恢复为默认设置。

⚠ 此设置将使系统变得不安全并面临受到攻击的风险。强烈建议在选择卸载之前先解决该选项删除补丁会导致的所有技术影响。

7. 在“Installation Completion（安装完成）”屏幕中选择 Finish（完成）。

ⓘ 如果需要验证安装报告，请参见*验证（第 4 页）*。

ⓘ 建议安装结束后重新启动。

验证

如果需要验证安装，可以查看生成的验证文件，其中包括日期和时间戳、安装的 Local Run Manager 版本以及其他关键验证值。要获得此文件，请联系 techsupport@illumina.com。

其他缓解措施和安全建议

RUO 仪器和 Dx 医疗设备的安全部署有赖于安全保护层。Illumina 强烈建议将仪器和设备与受信任的设备一起，部署在尽可能小的网络子网或安全环境中。此外，还非常建议使用防火墙和其他网络策略来限制其他入站和出站访问。

我们还建议：

- 启用传输层安全性协议 (TLS)，以确保所有仪器外通信都得到加密。
  - 要启用传输层安全性协议 (TLS)，请参见《Local Run Manager 软件指南》。

其他选项

如果因为某些原因无法选择执行该补丁，可以采用以下手动缓解方式来降低风险：

- 通过添加 Windows 防火墙规则来阻止使用端口 80 和 443 的传入连接，以禁用对 Local Run Manager 的远程访问。MSI 安装程序会在 Local Run Manager Web 服务器配置中自动阻止远程传入连接。能够达成同样效果的手动缓解措施是实施 Windows 防火墙配置，以阻止对 HTTP（TCP：80） 和 HTTPS（TLS、TCP：443）连接的传入连接。实施之后，只能在安装 Local Run Manager 的计算机上访问 Local Run Manager，无法再从连接到同一网络的其他计算机对其进行访问。

ⓘ 如果用户工作流程涉及远程访问 Local Run Manager，则此功能将不再起作用。

- 尽量减少其他网络设备的数量。

配置网络以尽量减少可与受影响的仪器进行通信的其他网络设备，会降低漏洞遭到利用的可能性。系统可用的连接越少，可供访问的机会就越少。
这可能需要咨询您当地的信息安全部门或 IT 人员才能实施。

- 将仪器断网。
  如果没有其他可行的方案，终极缓解措施是将仪器彻底断网。断网后将无法访问 Illumina 云/SaaS 服务（如 Proactive 和 BaseSpace® Sequence Hub）以及常规的基因组数据卸载工作流程。
  这可能需要咨询您当地的信息安全部门或 IT 人员才能实施。

对潜在未授权访问的调查

以下步骤可能有助于仪器操作员确定是否有未经授权的用户访问了系统：

1. 检查 C:\inetpub\logs\LogFiles\W3SVC1 中存储的 IIS 日志中是否存在异常调用。
   - 对 Local Run Manager Web 服务器的正常调用如下所示：

     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```

   - 对 Local Run Manager Web 服务器的异常调用举例如下：

     ```
     POST http /hackertool.asp
     ```

2. 检查 IIS 日志中是否有 POST 上载清单文件以外的内容的迹象。例如，以下调用将指示可疑活动：

   ```
   wscript
   shell
   wscript.network
   scripting.filesystemObject
   ```

3. 如果安装了防病毒/防恶意软件应用程序，请检查软件日志是否有异常行为迹象。
4. 检查 Windows 日志是否存在异常错误消息的迹象。
   如果威胁行为者获得管理员访问权限，他们将能更改或删除所有本地仪器日志和事件。

检查系统可能尝试访问过的任何端点。有关预期出站连接的列表，请参见控制计算机防火墙。

如需帮助，请联系 Illumina 技术支持。

修订历史记录

文档	日期	更改描述
文档号 200017330 v02	2022 年 4 月	添加了在仪器未运行时应用补丁的建议。 添加了在安装补丁后需要重新启动仪器的说明。 更正了 v01 的修订历史记录描述。
文档号 200017330 v01	2022 年 4 月	将文档标题更改为“LRM 软件补丁 1.0 说明指南”。 删除了文中提到的所有 v1.0.1。 添加了涵盖对潜在未授权访问的调查的章节。
文档号 200017330 v00	2022 年 3 月	初始版本。