LRM 軟體修補程式 1.0

illumina®

說明指南

簡介

Illumina® 近期發現 Local Run Manager 軟體有安全性漏洞，因此提供軟體修補程式防止該漏洞的遠端入侵攻擊。

Local Run Manager 為一套獨立軟體應用程式，且為以下系統的部分預設配置：

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

*供試管內診斷使用。

本指南適用於以上所列之 Illumina 儀器和已安裝 Local Run Manager 獨立版本的儀器外電腦。

此漏洞為未經授權的遠端指令執行（RCE），如未經緩解，CVSS 評分為重大風險 10 分，CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H。

下列緩解步驟在以上所列之儀器上均為必要措施，旨在阻絕未經授權之使用者存取一台或多台儀器和執行遠端存取攻擊的可能性。

如因故無法執行安裝程式，請查閱本文件最後的其他緩解方式一節，或聯絡 techsupport@illumina.com 取得額外協助。

請查閱取得 Local Run Manager 更新一節，了解下載或索取修補程式複本之方式的選項。

- **v1.0.0 修補程式** - 將更新 Local Run Manager 網頁設定，並停用遠端網際網路資訊服務（IIS）存取權。

取得 Local Run Manager 安全性修補程式

以下提供四（4）種取得 Local Run Manager 安全性修補程式的選項。

選項 1—直接下載至您的儀器

如欲取得 Local Run Manager 安全性更新，直接從支援網站下載至儀器最為快速。

1. 經由安全電子郵件所提供的連結，將修補程式安裝程式下載至您的儀器。
2. 將檔案傳輸至儀器的 C:\Illumina 資料夾。

3. 依照第 3 頁 *執行 Local Run Manager 安全性修補程式*的指示執行。

選項 2—請將修補程式安裝程式下載至電腦中，並透過 USB 隨身碟/共享資料夾將安裝程式傳輸至儀器。

如果您無法將安全性修補程式下載至儀器，建議您將其下載至個別電腦，再傳輸至儀器。

使用 USB 隨身碟前，請向資安人員驗證其完整性。(建議事項)

1. 經由安全電子郵件所提供的連結，將修補程式安裝程式下載至您的電腦或筆記型電腦。
2. 將已下載的修補程式安裝程式從該電腦複製到 USB 隨身碟或共享資料夾。
3. 如使用 USB 隨身碟，請將隨身碟插入儀器。
4. 從 USB 隨身碟或共享資料夾，將修補程式安裝程式複製到儀器的 C:\Illumina 資料夾。
5. 依照第 3 頁 *執行 Local Run Manager 安全性修補程式*的指示執行。

選項 3—請求技術支援

Illumina 技術支援人員將以下列其中一種方式引導您進行修補流程：

- 技術支援遠端登入
  技術支援人員將可會遠端存取分析儀，並代表客戶安裝修補程式。

  該系統必須可進行遠端存取。如您有任何疑問，請詢問當地 IT 人員以獲得協助。

- 指引說明
  技術支援人員將透過電話提供指引說明。請聯絡當地技術支援人員以獲得協助。

選項 4—向 Illumina 索取預先設定完成的隨身碟

客戶可免費索取一份具防寫保護的 USB 隨身碟。如欲索取內有修補程式的隨身碟，請聯絡 techsupport@illumina.com。

運送過程或庫存狀況皆可能影響投遞時效而造成延遲。為儘早保護系統，我們強烈建議應採取最具效率的解決途徑。

執行 Local Run Manager 安全性修補程式 v.1.0 安裝程式

執行 Illumina MSI (Microsoft Installer) 安裝程式時，將更新 Local Run Manager 網頁伺服器設定，防止任何使用者上傳內容執行，並封鎖所有從 LAN 遠端存取 Local Run Manager 網頁介面的網路連線。

對於使用 Local Run Manager 網頁介面遠端存取儀器的使用者而言，安裝此修補程式後，上述工作流程將無法繼續運作。Illumina 計畫稍後對此軟體問題進行永久性修正，以恢復上述功能。如既有工作流程因此中斷，請聯絡 techsupport@illumina.com 取得進一步協助。

MSI 安裝程式適用於各版本的 Local Run Manager，並能依儀器/電腦上所安裝的 Local Run Manager 版本自動判斷正確的修正檔。

這個 MSI 安裝程式也將建立一份稽核檔案，記錄此項緩解已經執行以及時間戳記，顯示安裝已確實完成。

執行 MSI 安裝程式—首次執行 MSI 安裝程式時，將進行系統修補，並建立一份包含完成時間的稽核檔案。

再次執行 MSI 安裝軟體時，將顯示［Repair（修復）］選項，使用者可選擇重新執行或取消安裝修補程式。注意：取消安裝修補程式將導致儀器設定不安全。

執行 Local Run Manager 安全性修補程式

安裝修補程式：

1. 以管理員帳戶（如 sbsadmin）登入系統。

   Illumina 建議您在儀器未執行時執行修補程式。如果儀器正在執行，則應在執行程序完成後，再立即執行修補程式。

2. 找出已下載至系統中的修補程式。
3. 將修補程式安裝程式移至 C:\Illumina 資料夾（免受軟體限制原則管制）。
4. 在安裝程式圖示上連按兩下即可啟動介面。
5. 應用程式載入後，請選取［Next（下一步）］開始安裝修補程式。
6. 請在安裝完成畫面選取［Finish（完成）］。

如需安裝報告驗證，請參閱第 4 頁 *驗證*一節。

安裝完畢後必須重新開機。

修復

如出現錯誤，客戶可依下列說明執行安裝修復作業：

1. 以管理員帳戶（如 sbsadmin）登入系統。
2. 找出已下載至系統中的修補程式。
3. 將修補程式安裝程式移至 C:\Illumina 資料夾（免受軟體限制原則管制）。
4. 在安裝程式圖示上連按兩下即可啟動介面。
5. 安裝程式將自動偵測設定工具是否曾經執行，並顯示新選項：
   a. 修改：顯示為灰色，不可使用
   b. 修復：修復錯誤並提供重新設定選項
   c. 移除：解除安裝修補程式，並恢復至預設設定（請參閱第 4 頁 *解除安裝*一節）
6. 請在安裝完成畫面選取［Finish（完成）］。

如需安裝報告驗證，請參閱第 4 頁 *驗證*一節。

安裝完畢後必須重新開機。

解除安裝

解除安裝修補程式將還原針對應用程式主機設定檔進行的修改項目。

1. 以管理員帳戶（如 sbsadmin）登入系統。
2. 找出已下載至系統中的修補程式。
3. 將修補程式安裝程式移至 C:\Illumina 資料夾（免受軟體限制原則管制）。
4. 在安裝程式圖示上連按兩下即可啟動介面。
5. 選取 [Remove（移除）]，解除安裝修補程式，並將所有設定值還原至預設設定。
6. 選取 [Remove（移除）]，驗證選項以解除安裝修補程式，並將所有設定值還原至預設設定。

⚠ 此設定將使系統處於不安全且可能遭受攻擊的狀態。強烈建議在選擇解除安裝前，先處理任何使您選擇移除修補程式的技術影響。

7. 請在安裝完成畫面選取 [Finish（完成）]。

ⓘ 如需安裝報告驗證，請參閱第 4 頁 *驗證*一節。

ⓘ 建議於安裝完畢後重新開機。

驗證

如需驗證安裝，可建立驗證檔案，其中包含日期和時間戳記、所安裝的 Local Run Manager 版本，以及其他重要驗證數值。請聯絡 techsupport@illumina.com 取得此檔案。

其他緩解方式和安全性相關建議

安全部署 RUO 儀器和 Dx 醫療器材取決於安全性階層。Illumina 強烈建議，儀器和器材連同受信任之設備，應部署於最小子網路或安全性環境中。採用防火牆和其他網路原則以限制其他輸入和輸出存取，係為適當措施。

此外，建議您：

- 啟用傳輸層安全性（TLS），確保所有儀器外通訊皆經過加密。
  - 若要啟用傳輸層安全性（TLS），請參閱「Local Run Manager 軟體指南」。

替代選項

如因故無法執行修補程式，以下手動緩解方法將可降低風險：

- 透過增加 Windows 防火牆規則，阻擋連入的連接埠 80 和 443 連線，藉此停用對 Local Run Manager 的遠端存取。MSI 安裝程式將在 Local Run Manager 網頁伺服器設定中，自動阻擋遠端連入連線。實施 Windows 防火牆設定也可達到相同效果，這個手動緩解措施會封鎖對 HTTP（TCP:80）和 HTTPS（TLS，TCP:443）連線的連入連線。一旦採取上述措施，Local Run Manager 便只能在原安裝電腦上存取，無法再透過連線至相同網路的其他電腦存取。

ⓘ 如使用者工作流程包含遠端存取 Local Run Manager，此功能將無法正常運作。

- 將其他網路裝置的數量減至最少。
  調整網路設定，將可與受影響儀器通訊的其他網路裝置數量減至最少，可降低遭受入侵攻擊的可能。可連接至系統的連線數越少，遭存取的可能性就越低。
  您可能需諮詢當地資訊安全人員或 IT 人員，以便執行上述措施。
- 將儀器從網路中移除。
  如果沒有其他選項可行，則最終的緩解措施為從網路中完全移除儀器。此舉將使您無法存取 Illumina Cloud/SaaS 服務（如 Proactive 和 BaseSpace® Sequence Hub），以及標準基因資料卸載工作流程。
  您可能需諮詢當地資訊安全人員或 IT 人員，以便執行上述措施。

潛在未經授權存取的調查

下列步驟可協助儀器操作員判斷未經授權之使用者是否已存取系統：

1. 檢查儲存於 C:\inetpub\logs\LogFiles\W3SVC1 的 IIS 記錄檔是否有異常呼叫。
   - 正常 Local Run Manager 網路伺服器呼叫如下所示：

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

   - 可能會出現異常 Local Run Manager 網路伺服器呼叫，如下所示：

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

2. 檢查 IIS 記錄檔是否有 POST 上傳非資訊清單檔案內容的徵兆。舉例來說，下列呼叫表示可疑活動：

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

3. 如果已安裝防毒/防惡意軟體應用程式，請查看軟體記錄檔是否有異常行為徵兆。
4. 檢查 Windows 記錄檔是否有異常錯誤訊息徵兆。
   如果威脅發動者已使用管理員權限存取，他們可修改或刪除所有本機儀器記錄檔和事件。

查看系統可能已嘗試存取的所有端點。如需預期向外連線清單，請參閱控制電腦防火牆。

必要時，請聯絡 Illumina 技術支援尋求協助。

修訂記錄

文件	日期	變更內容說明
文件編號 200017330 v02	2022 年 4 月	新增儀器未執行時執行修補程式的建議。 新增安裝修補程式後必須重新啟動儀器的指示。 修正 v01 的修訂記錄說明。
文件編號 200017330 v01	2022 年 4 月	已將文件標題變更為「LRM 軟體修補程式 1.0 說明指南」。 已移除提及 v1.0.1 的內容。 新增涵蓋潛在未經授權存取的調查一節。
文件編號 200017330 v00	2022 年 3 月	初版。