LRMソフトウェアパッチ1.0

illumina®

手順ガイド

はじめに

Illumina®では、Local Run Managerソフトウェアに存在するセキュリティの脆弱性を認識し、本脆弱性をリモートで悪用されないようにするためのソフトウェアパッチを提供しています。

Local Run Managerはスタンドアロンのソフトウェアアプリケーションであり、次のシステムの構成の一部となっています。

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

*本製品は体外診断の目的で使用されます。

本ガイドの適用対象は、上記のイルミナ装置と、スタンドアロン版のLocal Run Managerをインストールしている装置外のコンピューターです。

今回の脆弱性は、認証されていないリモートコマンド実行（Unauthenticated Remote Command Execution、RCE）です。CVSSスコアは10.0 Critical、`CVSS:3.1/CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`となっています。

1つまたは複数の装置にアクセスし、リモートアクセス攻撃を実行する可能性を防ぐために、以下の緩和措置が上記の装置で必須となっています。

何らかの理由でインストーラーが実行できない場合、本書の最後にある「その他の緩和措置」のセクションを参考にしていただくか、別途サポートが必要な場合はtechsupport@illumina.comまでお問い合わせください。

パッチのダウンロードやリクエストの方法については、「Local Run Managerセキュリティーパッチの取得」を参照してください。

- **v1.0.0パッチ：**Local Run Managerウェブ構成がアップデートされ、Internet Information Service (IIS)へのリモートアクセスが無効になります。

Local Run Managerセキュリティパッチの取得

Local Run Managerセキュリティパッチの入手方法には、4つのオプションがあります。

オプション1: 装置に直接ダウンロードする

Local Run Managerのセキュリティアップデートを取得する一番早い方法は、ウェブサイトからセキュリティアップデートを装置に直接ダウンロードすることです。

1. 安全なEメールにて提供されるリンクから、パッチインストーラーをお使いの装置にダウンロードします。
2. ファイルを、装置の`C:\Illumina`フォルダーに移動します。
3. 3ページの「Local Run Managerセキュリティパッチの適用」の手順に従います。

オプション2: パッチインストーラーをコンピューターにダウンロードして、USBドライブまたは共有フォルダー経由で装置に移動する

セキュリティパッチを装置にダウンロードできない場合は、別のコンピューターにダウンロードしてから装置に移すことをお勧めします。

USBドライブについては、使用する前に完全性に問題がないか、お客様の施設のセキュリティ担当者に確認してください。(推奨)

1. 安全なEメールにて提供されるリンクから、パッチインストーラーをお使いのコンピューターまたはノートパソコンにダウンロードします。
2. ダウンロードしたパッチインストーラーを、コンピューターからUSBドライブまたは共有フォルダーにコピーします。
3. USBドライブの場合、ドライブを装置に差し込みます。
4. USBドライブまたは共有フォルダーから、装置の`C:\Illumina`フォルダーにパッチインストーラーをコピーします。
5. 3ページの「Local Run Managerセキュリティパッチの適用」の手順に従います。

オプション3: テクニカルサポートに依頼する

イルミナのテクニカルサポート担当者が、次のいずれかの方法でパッチの適用作業を支援します。

- テクニカルサポートのリモートログイン

  テクニカルサポート担当者が解析装置にリモートでアクセスして、お客様の代わりにパッチをインストールします。

  システムはリモートアクセスが可能な状態にしておく必要があります。ご不明な点については、お客様の施設のIT担当者にご確認ください。

- 電話による説明

テクニカルサポート担当者が、電話にて手順を説明します。詳しくは、お近くのテクニカルサポート担当者にお問い合わせください。

オプション4: 事前設定済みのドライブをイルミナから注文する

書き込み禁止のUSBドライブを注文することも可能です。料金は無料です。パッチがインストールされたドライブを注文するには、techsupport@illumina.comにお問い合わせください。

出荷や在庫に遅延が発生すると、迅速な提供に影響を及ぼす可能性があります。システムをより早急に保護するために、最も効率的な解決法を提供してくれる手段でシステムを保護することを強く推奨します。

Local Run Managerセキュリティパッチv.1.0インストーラーの適用

Illumina MSI（Microsoftインストーラー）は、実行すると、Local Run Managerのウェブサーバー構成をアップデートし、ユーザーによりアップロードされたコンテンツの実行を防ぐとともに、LANネットワーク接続からLocal Run Managerウェブインターフェースへのあらゆるリモートアクセスをブロックします。

Local Run Managerウェブインターフェースを使用して各種装置にリモートでアクセスしているユーザーの場合、今回のパッチをインストールした後、このワークフローは機能しなくなります。この機能については、後日、今回の問題に対する永久的なソフトウェア修正にて復旧させる予定です。これによって、現在お使いのワークフローで中断が生じてしまう場合は、techsupport@illumina.comにご連絡ください。

MSIインストーラーは、すべてのバージョンのLocal Run Managerに適用可能で、装置またはコンピューターにインストールされているLocal Run Managerのバージョンに基づいて、適切な修正を自動で決定します。

また、このMSIインストーラーによって、この緩和措置が実装されたことを示す監査ファイルが、適切なインストールを反映するタイムスタンプと共に作成されます。

MSIインストーラーの実行：MSIインストーラーの初回実行時、インストーラーによってシステムにパッチが適用され、完了時刻が表記された監査ファイルが作成されます。

MSIインストーラーを再度実行すると、[**Repair**]オプションが表示され、パッチの再適用またはロールバックをすることができます。注:パッチをロールバックすると、装置の構成がセキュリティで保護されていない状態になります。

Local Run Managerセキュリティパッチの適用

パッチのインストール方法:

1. 管理者アカウント（例：sbsdmin）でシステムにログインします。

   装置が稼働していないときにパッチを適用することを推奨しています。
   装置がラン実行中の場合、ランの完了後すぐにパッチを適用してください。

2. システムにダウンロードされたパッチを見つけます。
3. パッチインストーラーを`C:\Illumina`フォルダーに移動します（ソフトウェア制限ポリシーの適用から除外されているフォルダー）。
4. インストーラーアイコンをダブルクリックして、インターフェースを起動します。
5. アプリケーションが読み込まれたら、[Next]を選択してパッチのインストールを開始します。
6. インストールの完了画面で[Finish]を選択します。

インストールの検証レポートが必要な場合は、5ページの「検証」を参照してください。

インストール終了時に再起動が必要です。

修復

エラーが発生した場合は、以下の手順に従って、インストールの修復作業を実行することができます。

1. 管理者アカウント（例：sbsdmin）でシステムにログインします。
2. システムにダウンロードされたパッチを見つけます。
3. パッチインストーラーを`C:\Illumina`フォルダーに移動します（ソフトウェア制限ポリシーの適用から除外されているフォルダー）。
4. インストーラーアイコンをダブルクリックして、インターフェースを起動します。
5. 構成ツールが以前に実行されたことがないかインストーラーが自動で検出し、新しいオプションが表示されます。
   a. Change:グレーアウトされており、使用できません
   b. Repair:エラーを修復し、再構成のオプションを利用できます。
   c. Remove:パッチをアンインストールし、初期設定の構成に戻します（4ページの「アンインストール」を参照）。
6. インストールの完了画面で［Finish］を選択します。

インストールの検証レポートが必要な場合は、4ページの「検証」を参照してください。

インストール終了時に再起動が必要です。

アンインストール

パッチのアンインストールを行うと、アプリケーションのホスト構成ファイルに加えられた変更内容が元の状態に戻ります。

1. 管理者アカウント（例：sbsdmin）でシステムにログインします。
2. システムにダウンロードされたパッチを見つけます。
3. パッチインストーラーを`C:\Illumina`フォルダーに移動します（ソフトウェア制限ポリシーの適用から除外されているフォルダー）。
4. インストーラーアイコンをダブルクリックして、インターフェースを起動します。
5. ［Remove］を選択してパッチをアンインストールし、すべての値を初期設定に戻します。
6. ［Remove］を選択してパッチをアンインストールするオプションを検証し、すべての値を初期設定に戻します。

この設定にすると、システムがセキュリティで保護されていない状態になり、攻撃を受ける危険性があります。アンインストールを選ぶ前に、パッチの削除が必要になった技術的な影響にすべて対処しておくことが強く推奨されます。

7. インストールの完了画面で［**Finish**］を選択します。

インストールの検証レポートが必要な場合は、4ページの「検証」を参照してください。

インストール終了時に再起動が必要です。

検証

インストールの検証が必要な場合は、日付、タイムスタンプ、インストールされているLocal Run Managerのバージョンなどの重要な検証値が含まれる検証ファイルをご利用いただけます。このファイルを取得するには、techsupport@illumina.comまでお問い合わせください。

その他の緩和措置およびセキュリティの推奨事項

研究用(RUO)装置や診断(Dx)医療機器の安全な導入は、何層ものセキュリティに依存します。イルミナでは、各種装置や機器を、その他の信頼できる機器と共に、最小のネットワークサブネットまたはセキュリティコンテキストに展開することを強く推奨します。ファイアウォールおよびその他のネットワークポリシーを用いて、その他のインバウンドおよびアウトバウンドのアクセスを制限することも強く推奨します。

その他の推奨事項は次のとおりです。

- トランスポート層セキュリティ(TLS)を有効にする:装置外の通信はすべて暗号化されます。
  - トランスポート層セキュリティ(TLS)を有効にする手順については、『Local Run Manager Software Guide』を参照してください。

代替措置

何らかの理由でパッチを実行することができない場合、以下に挙げる手動の緩和措置を行うとリスクが低減されます。

- ポート80および443の着信接続をブロックするWindowsファイアウォールルールを追加して、Local Run Managerへのリモートアクセスを無効にする。
  MSIによって、リモートの着信接続はLocal Run Managerウェブサーバー構成内で自動的にブロックされます。手動の緩和措置で同じ結果を可能にするためには、`HTTP(TCP:80)`への着信接続および`HTTPS(TLS、TCP:443)`接続をブロックするWindowsファイアウォール構成を実装します。
  実装が完了すると、Local Run Managerへのアクセスは、Local Run Managerがインストールされているコンピューター上でのみ可能になり、同じネットワークに接続されているその他のコンピューターからはアクセスできなくなります。

  ユーザーのワークフローでLocal Run Managerへのリモートアクセスが必要な場合、そのための機能が動作しなくなります。

- その他のネットワークデバイスの数を最小限にする。

  影響のある装置に通信できるその他のネットワークデバイスの数が最小限になるようにネットワークを構成することで、不正アクセスの可能性を減らすことができます。システムに接続できる数が少なければ、アクセスできる機会も少なくなるというわけです。
  この措置を実行するには、お客様の施設の情報セキュリティ担当者またはIT担当者との相談が必要な場合があります。

- ネットワークから装置を削除する。

  他のオプションが実行不可能な場合、最終手段は、ネットワークから装置を完全に削除することです。ただし、これを実行すると、ProactiveやBaseSpace® Sequence Hubといったイルミナのクラウドおよびサービスや、典型的なゲノムデータのオフロードワークフローへのアクセスが無効になります。
  この措置を実行するには、お客様の施設の情報セキュリティ担当者またはIT担当者との相談が必要な場合があります。

不正アクセスの可能性がある場合の調査

次のステップは、装置のオペレーターが不正なユーザーがシステムにアクセスしたかどうかを判断する上で役に立つ場合があります。

1. `C:\inetpub\logs\LogFiles\W3SVC1`に格納されているIISログを精査して、異常な呼び出しの有無を確認します。
   - Local Run Managerウェブサーバーへの正常な呼び出しは、例えば次のように表示されます。

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

   - Local Run Managerウェブサーバーへの異常な呼び出しは、次のように表示されます。

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

2. IISログを精査して、マニフェストファイルではなく、コンテンツのPOSTアップロードの兆候の有無を確認します。例えば、次の呼び出しは疑わしい活動を意味します。

```
wscript

shell

wscript.network

scripting.filesystemObject
```

3. ウイルス対策およびマルウェア対策アプリケーションがインストールされている場合は、ソフトウェアのログで異常な挙動の兆候の有無を確認します。
4. Windowsのログを精査して、異常なエラーメッセージの兆候の有無を確認します。
   不正なユーザーが管理者権限でアクセスに成功した場合、ローカルのすべての装置のログやイベントを書き換えたり削除したりすることが可能になります。

アクセスを試みた可能性があるすべてのエンドポイントについて確認します。期待される送信接続の一覧については、「制御コンピューターのファイアフォール」を参照してください。

お困りの場合は、必要に応じてイルミナのテクニカルサポートまでお問い合わせください。

改訂履歴

文書	日付	変更内容
文書番号 200017330 v02	2022年4月	装置がランしていない時にパッチを適用することを推奨する旨を追記。 パッチインストール後、装置の再起動が必要であることを追記。 v01の改訂履歴の記述を修正。
文書番号 200017330 v01	2022年4月	文書のタイトルを「LRMソフトウェアパッチ1.0手順ガイド」に変更。 v1.0.1に関する記述をすべて削除。 不正アクセスの可能性の調査に関するセクションを追加。
文書番号 200017330 v00	2022年3月	初版。

本製品は体外診断の目的で使用されます。

本製品の使用目的は研究に限定されます。診断での使用はできません。