# Софтуерна корекция 1.0 на LRM

illumina®

Ръководство с инструкции

# Въведение

В Illumina® научихме за уязвимост в сигурността, присъстваща в софтуера Local Run Manager, и предоставихме софтуерна корекция за защита срещу отдалеченото използване на тази уязвимост.

Local Run Manager е самостоятелно софтуерно приложение и част от конфигурацията по подразбиране на следните системи:

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

*За инвитро диагностична употреба.

Това ръководство се отнася за инструментите на Illumina, посочени по-горе, и също за компютри извън инструмента, които имат инсталирана самостоятелна версия на Local Run Manager.

Уязвимостта е изпълнение на неоторизирана отдалечена команда (RCE) с несмекчен CVSS резултат от 10,0 – критичен,`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Следните стъпки за смекчаване са необходими на всички инструменти, посочени по-горе, за да се предпазите от възможността неупълномощен потребител да получи достъп до един или повече инструменти и да извърши атака с отдалечен достъп.

Ако по някаква причина инсталаторът не може да се стартира, вижте раздела за допълнителни смекчавания в края на този документ или се свържете с techsupport@illumina.com за допълнително съдействие.

Вижте Получаване на актуализацията на Local Run Manager за опции как да изтеглите или поискате копие на корекцията.

- **корекция v1.0.0** – ще актуализира уеб конфигурацията на Local Run Manager и ще дезактивира отдалечения достъп до Internet Information Services (IIS).

# Получаване на корекцията за защита на Local Run Manager

Има четири (4) опции за получаване на корекцията за защита на Local Run Manager.

**Опция 1 – Изтеглете директно на инструмента**

Най-бързият начин да получите актуализацията за сигурност на Local Run Manager е да я изтеглите директно от хостващия уебсайт на инструмента.

1. Изтеглете инсталатора на корекцията от предоставената връзка чрез защитен имейл на вашия инструмент.
2. Прехвърлете файла в папката `C:\Illumina` на инструмента.
3. Следвайте инструкциите в *Прилагане на корекцията за защита на Local Run Manager* на страница 4.

**Опция 2 – Изтеглете инсталатора на корекцията на компютъра и го прехвърлете на инструмента чрез USB устройство/споделена папка**

Ако не можете да изтеглите корекцията за защита на инструмента, препоръчваме да я изтеглите на отделен компютър и след това да я прехвърлите на инструмента.

Потвърдете целостта на USB устройството с представители от отдела за сигурност, преди да го използвате (препоръчва се).

1. Изтеглете инсталатора на корекция от предоставената връзка чрез защитен имейл на вашия компютър или лаптоп.
2. Копирайте изтегления инсталатор на корекция на USB устройството или споделената папка от компютъра.
3. За USB устройство включете устройството в инструмента.
4. Копирайте инсталатора на корекция от USB устройството или споделената папка в папката `C:\Illumina` на инструмента.
5. Следвайте инструкциите в *Прилагане на корекцията за защита на Local Run Manager* на страница 4.

**Опция 3 – Поискайте техническа поддръжка**

Представител от отдела за техническа поддръжка на Illumina ще ви преведе през процеса на корекция, като използва един от следните методи:

- Отдалечено влизане за техническа поддръжка

  Представител от отдела за техническа поддръжка ще получи достъп до анализатора чрез отдалечен достъп и ще инсталира корекцията от името на клиента.

  Системата трябва да бъде достъпна от разстояние. Ако имате въпроси, обърнете се към местния ИТ представител за съдействие.

- Инструкции с насоки
  Представител от отдела за техническа поддръжка ще предостави инструкции с насоки по телефона. Свържете се с местния представител от отдела за техническа поддръжка за съдействие.

**Опция 4 – Поръчайте предварително конфигурирано устройство от Illumina**

Клиентът може да поръча безплатно USB устройства, защитени срещу запис. За да поръчате устройството с инсталирана корекция, свържете се с techsupport@illumina.com.

Възможно е да има закъснения на пратки или инвентар, които могат да повлияят на навременността на доставката. За да защитите системите по-скоро, силно се препоръчва те да бъдат защитени по метода, който ще предложи най-ефективния път за разрешаване.

# Прилагане на инсталатора за корекция за защита v.1.0 на Local Run Manager

Когато се изпълни, Illumina MSI (инсталатор на Microsoft) ще актуализира конфигурацията на уеб сървъра на Local Run Manager, за да предотврати изпълнението на всяко качено от потребителя съдържание и да блокира целия отдалечен достъп до уеб интерфейса на Local Run Manager от LAN мрежови връзки.

За потребителите, които използват уеб интерфейса на Local Run Manager за отдалечен достъп до инструменти, този работен процес ще престане да функционира след инсталирането на корекцията. Illumina възнамерява да възстанови функционалността с постоянната софтуерна корекция за този проблем по-късно. Ако това причини прекъсване на установените работни процеси, свържете се с techsupport@illumina.com за допълнително съдействие.

Инсталаторът MSI е приложим за всички версии на Local Run Manager и автоматично ще определи правилната корекция въз основа на версията на Local Run Manager, инсталирана на инструмента/компютъра.

Този инсталатор MSI също така ще създаде одитен файл, показващ, че този метод за смекчаване е приложен заедно с времево клеймо, което отразява правилната инсталация.

Изпълнение на инсталатор MSI – при първото стартиране на инсталатора MSI той ще коригира системата и ще създаде одитен файл с времето за завършване.

Стартирането на инсталатора MSI отново ще представи опция **Repair** (Поправка), на потребителя се дава възможност да приложи отново или да върне корекцията. Забележка: връщането на корекцията ще доведе до несигурна конфигурация на инструмента.

# Прилагане на корекцията за защита на Local Run Manager

**За да инсталирате корекцията:**

1. Влезте в системата чрез администраторски акаунт (напр. sbsadmin).

   Illumina препоръчва корекцията да се приложи, когато инструментът не се изпълнява. Ако инструментът извърша изпълняване, корекцията трябва да се приложи веднага след приключване на изпълняването.

2. Намерете корекцията, която е била изтеглена в системата.
3. Преместете инсталатора на корекцията в папката `C:\Illumina` (изключена от правилата за софтуерни ограничения).
4. Щракнете двукратно върху иконата на инсталатора, за да стартирате интерфейса.
5. Когато приложението се зареди, изберете **Next** (Напред), за да започнете инсталирането на корекцията.
6. На екрана за завършване на инсталацията изберете **Finish** (Край).

В случай че е необходим доклад за потвърждаване на инсталирането, вижте *Потвърждаване* на страница 5.

Изисква се рестартиране в края на инсталацията.

**Поправка**

В случай на грешка клиентът може да извърши поправка на инсталацията, като следва инструкциите по-долу:

1. Влезте в системата чрез администраторски акаунт (напр. sbsadmin).
2. Намерете корекцията, която е била изтеглена в системата.
3. Преместете инсталатора на корекцията в папката `C:\Illumina` (изключена от правилата за софтуерни ограничения).
4. Щракнете двукратно върху иконата на инсталатора, за да стартирате интерфейса.
5. Инсталаторът автоматично ще открие дали инструментът за конфигуриране е бил изпълняван преди и ще представи нови опции:
   a. Change (Промяна): оцветена в сиво и недостъпна.
   b. Repair (Поправка): поправя грешки и дава опции за преконфигуриране.
   c. Remove (Премахване): деинсталира корекцията и я възстановява до конфигурацията по подразбиране (вж. *Деинсталиране* на страница 5)
6. На екрана за завършване на инсталацията изберете **Finish** (Край).

В случай че е необходим доклад за потвърждаване на инсталирането, вижте *Потвърждаване* на страница 5.

Изисква се рестартиране в края на инсталацията.

**Деинсталиране**

Деинсталирането на корекцията връща промените, направени в конфигурационния файл на хоста на приложението.

1. Влезте в системата чрез администраторски акаунт (напр. sbsadmin).
2. Намерете корекцията, която е била изтеглена в системата.
3. Преместете инсталатора на корекцията в папката `C:\Illumina` (изключена от правилата за софтуерни ограничения).
4. Щракнете двукратно върху иконата на инсталатора, за да стартирате интерфейса.
5. Изберете **Remove** (Премахване), за да деинсталирате корекцията и да върнете всички стойности към настройките по подразбиране.
6. Изберете **Remove** (Премахване), за да потвърдите опцията за деинсталиране на корекцията и да върнете всички стойности към настройките по подразбиране.

Тази настройка ще направи системата несигурна и изложена на риск от атака. Силно препоръчително е да обърнете внимание на всички технически въздействия, до които води опцията за премахване на корекцията, преди да решите да деинсталирате.

7. На екрана за завършване на инсталацията изберете **Finish** (Край).

В случай че е необходим доклад за потвърждаване на инсталирането, вижте *Потвърждаване* на страница 5.

Препоръчва се рестартиране в края на инсталацията.

**Потвърждаване**

Ако има нужда от потвърждаване на инсталацията, ще бъде генериран файл за потвърждаване, който включва времево клеймо с дата и час, инсталирана версия на Local Run Manager и други ключови стойности за потвърждение. За да получите този файл, свържете се с techsupport@illumina.com.

# Допълнителни препоръки за смекчаване и сигурност

Сигурното внедряване на инструменти в RUO и диагностични (Dx) медицински изделия зависи от слоевете на сигурност. Illumina силно препоръчва инструментите и устройствата да се внедряват в най-малката подмрежа или контекст на сигурността с доверени устройства. Използването на защитни стени

и други мрежови правила за ограничаване на друг входящ и изходящ достъп е силно препоръчително.

Ние препоръчваме и:

- Активирайте защитата на транспортния слой (TLS), за да гарантирате, че всички комуникации извън инструмента са шифровани.
  - За да активирате защитата на транспортния слой (TLS), вижте софтуерното ръководство за Local Run Manager.

# Алтернативни опции

Ако по някаква причина изпълнението на корекцията не е опция, следните ръчни методи за смекчаване ще намалят риска:

- Дезактивирайте отдалечения достъп до Local Run Manager, като добавите правила за защитната стена на Windows, за да блокирате входящите връзки на порт 80 и 443.
  Инсталаторът MSI автоматично ще блокира отдалечени входящи връзки в конфигурацията на уеб сървъра на Local Run Manager. Ръчен метод за смекчаване, който постига същия резултат, е да се внедри конфигурация на защитната стена на Windows за блокиране на входящи връзки към `HTTP (TCP:80)` и `HTTPS (TLS, TCP:443)`.
  След внедряването Local Run Manager може да бъде достъпен само на компютъра, на който е инсталиран; вече няма да е достъпен от други компютри, свързани към същата мрежа.

  Ако работният процес на потребителя включва отдалечен достъп до Local Run Manager, тази функционалност вече няма да работи.

- Минимизирайте броя на другите мрежови устройства.
  Конфигурирането на мрежата за минимизиране на броя на други мрежови устройства, които могат да комуникират със засегнатия инструмент, ще намали възможността за експлоатацията. Колкото по-малко връзки са налични към системата, толкова по-малко възможности има за достъп. Изпълнението на това може да изисква консултация с местния ви отдел по информационна сигурност или ИТ ресурси.
- Отстранете инструмента от мрежата.
  Ако не е възможна друга опция, последният метод за смекчаване е да премахнете изцяло инструмента от мрежата. Това ще дезактивира достъпа до услуги Illumina Cloud/SaaS, като Proactive и BaseSpace® Sequence Hub, и типичните работни процеси за разтоварване на геномни данни. Изпълнението на това може да изисква консултация с местния ви отдел по информационна сигурност или ИТ ресурси.

# Разследване на потенциален неупълномощен достъп

Следните стъпки могат да помогнат на оператора на инструмента да определи дали неупълномощен потребител е получил достъп до системата:

1. Прегледайте регистрите на IIS, съхранени в `C:\inetpub\logs\LogFiles\W3SVC1`, за анормални извиквания.
   - Нормалните извиквания към уеб сървъра на Local Run Manager се показват, както следва:

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

   - Анормалните извиквания към уеб сървъра на Local Run Manager може да се показват, като например, както следва:

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

2. Прегледайте регистъра на IIS за признаци на качвания с POST на съдържание, различно от манифестни файлове. Следните извиквания например биха показали подозрителна активност:

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

3. Ако е инсталирано антивирусно приложение или такова против злонамерен софтуер, проверете регистрите му за признаци на анормално поведение.
4. Прегледайте регистрите на Windows за признаци на анормални съобщения за грешка.
   Ако даден извършител, който се възползва от заплахата, получи достъп с администраторски права, той би могъл да промени или изтрие всички локални регистри и събития на инструмента.

Проверете за крайни точки, до които системата може да се е опитала да получи достъп. Вижте Защитна стена на контролния компютър за списък с очаквани изходящи връзки.

Свържете се с отдела за техническа поддръжка на Illumina за съдействие при необходимост.

# Хронология на редакциите

| Документ | Дата | Описание на промяната |
|---|---|---|
| Документ № 200017330 v02 | Април 2022 г. | Добавена е препоръка за прилагане на корекция, когато инструментът не се изпълнява.<br>Добавена е инструкция, че е необходимо рестартиране на инструмента след инсталиране на корекция.<br>Коригирано е описанието на хронологията на редакциите за v01. |
| Документ № 200017330 v01 | Април 2022 г. | Променено заглавие на документа на Ръководство с инструкции за софтуерна корекция 1.0 на LRM.<br>Премахнато споменаване на v1.0.1.<br>Добавен е раздел, който обхваща разследването на потенциален неупълномощен достъп. |
| Документ № 200017330 v00 | Март 2022 г. | Първоначална версия. |