# Программное исправление версии 1.0 для LRM

illumina®

## Пошаговые инструкции

# Введение

Компании Illumina® стало известно об уязвимости средств безопасности программного обеспечения Local Run Manager, и она выпустила исправление программного обеспечения для защиты от удаленного ненадлежащего использования данной уязвимости.

Local Run Manager представляет собой автономное программное приложение и является частью конфигурации по умолчанию следующих систем:

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

* Для диагностики in vitro.

Это руководство применимо к перечисленным выше приборам Illumina и внешним компьютерам, на которых установлена автономная версия Local Run Manager.

Уязвимость представляет собой неаутентифицированное удаленное исполнение команды (RCE, Remote Command Execution) с исходной оценкой по стандарту оценки уязвимости (CVSS), равной 10.0 (критическая), `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Необходимы указанные далее шаги по снижению рисков в отношении вышеперечисленных приборов для защиты от возможного доступа несанкционированного пользователя к одному или более приборам с целью атаки с помощью удаленного доступа.

Если по какой-либо причине установщик невозможно запустить, обратитесь к разделу по дополнительным мерам снижения рисков в конце этого документа или по адресу techsupport@illumina.com для получения дополнительной помощи.

В разделе Получение обновления Local Run Manager приведены варианты загрузки или запроса копии исправления.

- **Исправление v1.0.0** — обновляет веб-конфигурацию Local Run Manager и отключает удаленный доступ к службам информационного сервера интернета (Internet Information Services, IIS).



**Исключительно для использования в научно-исследовательских целях.**
**Не предназначено для использования в диагностических процедурах.**

# Получение обновления системы безопасности Local Run Manager

Существует 4 (четыре) варианта обновления системы безопасности Local Run Manager.

**Вариант 1: скачайте обновление на прибор напрямую**

Наиболее быстрый путь получить обновление безопасности для Local Run Manager Security Update — скачать его непосредственно с веб-сайта на прибор.

1. Скачайте установщик исправления по предоставленной через защищенную электронную почту ссылке на свой прибор.
2. Переместите файл в папку `C:\Illumina` прибора.
3. Следуйте инструкциям в разделе *Применение исправления безопасности для Local Run Manager* на стр. 4.

**Вариант 2: скачайте установщик исправления на компьютер и перенесите его в прибор с помощью USB-накопителя / папки совместного использования**

Если вы не можете скачать обновление системы безопасности, мы рекомендуем скачать его на отдельный компьютер, а затем перенести на прибор.

Прежде чем использовать USB-накопитель, проверьте его работоспособность вместе с представителями отдела безопасности. (Рекомендуется.)

1. Скачайте установщик исправления по предоставленной через защищенную электронную почту ссылке на свой компьютер или ноутбук.
2. Скопируйте скачанный установщик исправления с компьютера на USB-накопитель или в папку совместного использования.
3. При использовании USB-накопителя подключите его к прибору.
4. Скопируйте установщик исправления с USB-накопителя или из папки с общим доступом в папку `C:\Illumina` на приборе.
5. Следуйте инструкциям в разделе *Применение исправления безопасности для Local Run Manager* на стр. 4.

**Вариант 3: обратитесь в техническую поддержку**

Представитель отдела технической поддержки компании Illumina проведет вас через процесс внедрения изменения с помощью одного из приведенных ниже методов.

- Удаленный доступ технической поддержки

  Представитель отдела технической поддержки получает удаленный доступ к анализатору и устанавливает исправление от имени заказчика.

Система должна поддерживать удаленный доступ. В случае любых вопросов обратитесь за помощью к представителю местного отдела ИТ.

- Пошаговые инструкции

  Представитель технической поддержки предоставляет пошаговые инструкции по телефону. Обратитесь за помощью к вашему местному представителю технической поддержки.

**Вариант 4: закажите предварительно настроенный накопитель в Illumina**

Клиенты могут бесплатно заказать защищенные от записи USB-накопители. Для заказа накопителя с установленным исправлением обратитесь по адресу techsupport@illumina.com.

Задержки с поставками или отсутствие на складе могут повлиять на своевременность доставки. Для более быстрой защиты систем настоятельно рекомендуется защищать их с использованием метода, который обеспечит наиболее эффективный путь решения проблемы.

# Применение установщика исправления системы безопасности v.1.0 для Local Run Manager

В результате запуска Illumina MSI (установщик Microsoft) происходит обновление конфигурации веб-сервера Local Run Manager с целью предотвращения выполнения загруженного пользователями содержимого и блокировки удаленного доступа подключений из сети LAN к веб-интерфейсу Local Run Manager.

После установки этого исправления пользователи, использующие веб-интерфейс Local Run Manager для удаленного доступа к приборам, потеряют такую возможность. Illumina планирует восстановить эту функцию позже с помощью постоянного исправления программного обеспечения для решения этой проблемы. Если это действие приведет к прерыванию установленных рабочих процессов, обратитесь за помощью по адресу techsupport@illumina.com.

Установщик MSI применим ко всем версиям Local Run Manager, и он автоматически определит использование необходимого исправления на основании версии Local Run Manager, установленной на приборе/компьютере.

Этот установщик MSI также создаст файл истории аудита, демонстрирующий, что эта мера по снижению риска была применена, с отметкой времени для отражения момента правильной установки.

Запуск установщика MSI: при первом запуске установщик MSI внедрит исправление в систему и создаст файл истории аудита с указанием времени выполнения этого действия.

При повторном запуске установщик MSI предоставит вариант **Repair** (Исправить), и пользователю будет предоставлен выбор между повторным применением или откатом исправления. Примечание. Откат исправления приведет к небезопасной конфигурации прибора.

# Применение исправления безопасности для Local Run Manager

**Для установки исправления**

1. Войдите в систему через учетную запись администратора (например, sbsadmin).

   Компания Illumina рекомендует применять исправление тогда, когда прибор не работает. Если прибор работает, исправление необходимо применить сразу же после завершения работы.

2. Найдите исправление, которое было скачано в систему.
3. Переместите установщик исправления в папку `C:\Illumina` (исключение из «Политики ограниченного использования программ»).
4. Дважды нажмите на иконку установщика для запуска интерфейса.
5. Когда приложение будет загружено, нажмите **Next (Далее)**, чтобы начать установку исправления.
6. На экране Installation Completion (Завершение установки) нажмите **Finish** (Завершить).

В случае если требуется верификация отчета об установке, см. пункт *Верификация* на стр. 5.

По завершении установки необходимо выполнить перезагрузку.

**Восстановление**

В случае ошибки клиент может выполнить восстановление установки, следуя инструкциям ниже.

1. Войдите в систему через учетную запись администратора (например, sbsadmin).
2. Найдите исправление, которое было скачано в систему.
3. Переместите установщик исправления в папку `C:\Illumina` (исключение из «Политики ограниченного использования программ»).
4. Дважды нажмите на иконку установщика для запуска интерфейса.
5. Установщик автоматически определит, запускался ли инструмент для конфигурирования ранее, и предоставит новые варинаты.
   a. Change (Изменить): выделено серым цветом и недоступно.
   b. Repair (Восстановить): исправляет ошибки и предоставляет варианты для изменения конфигурации.
   c. Remove (Удалить): удаляет исправление и восстанавливает конфигурацию по умолчанию (см. пункт *Удаление* на стр. 5).

6. На экране Installation Completion (Завершение установки) нажмите **Finish** (Завершить).

> В случае если требуется верификация отчета об установке, см. пункт *Верификация* на стр. 5.

> По завершении установки необходимо выполнить перезагрузку.

**Удаление**

Удаление исправления откатывает изменения в файле конфигурации хоста приложения.

1. Зайдите в систему через учетную запись администратора (например, sbsadmin).
2. Найдите исправление, которое было скачано в систему.
3. Переместите установщик исправления в папку `C:\Illumina` (исключение из «Политики ограниченного использования программ»).
4. Дважды нажмите на иконку установщика для запуска интерфейса.
5. Нажмите **Remove** (Удалить), чтобы удалить исправление и вернуть все значения к настройкам по умолчанию.
6. Нажмите **Remove** (Удалить), чтобы верифицировать вариант удаления исправления и вернуть все значения к настройкам по умолчанию.

> Эта настройка сделает систему небезопасной и подвергнет ее риску атак. Настоятельно рекомендуется устранить любые технические моменты, спровоцировавшие рассмотрение опции удаления исправления, прежде чем принять решение об удалении.

7. На экране Installation Completion (Завершение установки) нажмите **Finish** (Завершить).

> В случае если требуется верификация отчета об установке, см. пункт *Верификация* на стр. 5.

> По завершении установки рекомендуется перезагрузка.

**Верификация**

В случае необходимости верифицировать установку будет создан файл верификации, включающий метку даты и времени, установленную версию Local Run Manager и другие ключевые значения верификации. Для получения этого файла обратитесь по адресу techsupport@illumina.com.

# Дополнительные рекомендации по снижению рисков и обеспечению безопасности

Безопасный запуск приборов, предназначенных для научно-исследовательских целей (RUO), и диагностических медицинских устройств зависит от уровней безопасности. Компания Illumina настоятельно рекомендует, чтобы ввод приборов и устройств в эксплуатацию осуществлялся в подсети минимального размера или в среде безопасности с надежными устройствами. Настоятельно рекомендуется использовать брандмауэры и другие политики сети для ограничения прочего входящего и исходящего доступа.

Мы также рекомендуем выполнить указанные далее действия.

- Активируйте протокол Transport Layer Security (TLS) для обеспечения шифрования всех соединений вне прибора.
  - Процедура активации протокола Transport Layer Security (TLS) описана в руководстве по программному обеспечению Local Run Manager.

# Альтернативные варианты

Если по какой-либо причине внедрение исправления не представляется возможным, уменьшить уровень риска позволят следующие методы по снижению риска вручную.

- Отключите удаленный доступ к Local Run Manager, добавив правила брандмауэра Windows для блокировки входящих подключений через порты 80 и 443.
  Установщик MSI будет автоматически блокировать удаленные входящие подключения в конфигурации веб-сервера Local Run Manager. Тот же результат обеспечивает применение конфигурации брандмауэра Windows для блокировки входящих подключений к соединениям `HTTP (TCP:80)` и `HTTPS (TLS, TCP:443)`.
  После применения доступ к программному обеспечению Local Run Manager будет открыт только на компьютере, на котором оно установлено; оно больше не будет доступно с других компьютеров, подключенных к той же сети.

> Если рабочий процесс пользователя предусматривает удаленный доступ к Local Run Manager, эта функция больше не будет работать.

- Сведите к минимуму использование других сетевых устройств.

Создание конфигурации сети, в которой сведено к минимуму количество других сетевых устройств, которые могут подключаться к затронутому прибору, снизит возможность неправомерного использования. Чем меньше подключений доступно в системе, тем меньше возможностей для доступа.
Для выполнения этого действия может потребоваться консультация с местными службами информационной безопасности или специалистами ИТ-отдела.

- Исключите прибор из сети.
  В случае отсутствия других практически осуществимых вариантов окончательным способом снижения риска является полное исключение прибора из сети. В этом случае будет отключен доступ к службам Illumina Cloud/SaaS, таким как Proactive и BaseSpace® Sequence Hub, а также к типовым рабочим процессам выгрузки геномных данных.
  Для выполнения этого действия может потребоваться консультация с местными службами информационной безопасности или специалистами ИТ-отдела.

# Расследование возможного несанкционированного доступа

Указанные далее шаги могут помочь оператору прибора определить, имел ли место доступ в систему несанкционированного пользователя.

1. Проверьте журналы информационного интернет-сервера, которые хранятся по адресу `C:\inetpub\logs\LogFiles\W3SVC1`, на предмет ненадлежащих вызовов.
   - Обычные вызовы веб-сервера Local Run Manager выглядят так:
     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```
   - Ненадлежащие вызовы веб-сервера Local Run Manager выглядят так:
     ```
     POST http /hackertool.asp
     ```
2. Проверьте журналы информационного интернет-сервера на наличие признаков загрузок методом POST контента, который не является файлами манифеста. Например, такие вызовы указывают на подозрительную активность:
   ```
   wscript
   shell
   wscript.network
   scripting.filesystemObject
   ```
3. Если установлена программа-антивирус, проверьте файлы журналов на наличие признаков ненормального поведения.

4. Проверьте журналы Windows на наличие ненормальных сообщений об ошибках.
   Если злоумышленник получил доступ к правам администратора, у него была возможность изменить или удалить все локальные журналы и события прибора.

Проверьте все конечные точки, к которым пробовала подключиться система. Список ожидаемых внешних подключений см. в брандмауэре управляющего компьютера.

При необходимости обратитесь за помощью в службу технической поддержки компании Illumina.

# История изменений

| Документ | Дата | Описание изменений |
|---|---|---|
| Документ № 200017330 v02 | Апрель 2022 г. | Добавлена рекомендация по применению исправления тогда, когда прибор не работает.<br>Добавлена рекомендация о необходимости перезагрузки прибора по завершении установки.<br>Исправлено описание истории изменений для v01. |
| Документ № 200017330 v01 | Апрель 2022 г. | Название документа изменено на «Пошаговые инструкции к программному исправлению версии 1.0 для LRM».<br>Удалены упоминания версии 1.0.1.<br>Добавлен раздел, описывающий расследование возможного несанкционированного доступа. |
| Документ № 200017330 v00 | Март 2022 г. | Первый выпуск. |

Настоящий документ и его содержание являются собственностью компании Illumina, Inc. и ее аффилированных лиц (Illumina) и предназначены для использования исключительно в рамках договора заказчиком при эксплуатации изделия (-й), описанного (-ых) в настоящем документе, и ни для какой иной цели. Настоящий документ и его содержание не подлежат использованию или распространению не по назначению и/или передаче, раскрытию или воспроизведению каким-либо способом без предварительного письменного согласия компании Illumina. Настоящим документом компания Illumina не передает никаких лицензий на свои патенты, товарные знаки, авторские права или права, признаваемые общим правом, или аналогичные права третьих лиц.

Инструкции, изложенные в настоящем документе, должны строго и точно соблюдаться квалифицированным и прошедшим соответствующее обучение персоналом для обеспечения правильной и безопасной эксплуатации изделий, описанных в настоящем документе. Перед использованием такого изделия (-й) необходимо в полном объеме прочитать и понять всю информацию, представленную в этом документе.

НЕВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ПО ПОЛНОМУ ПРОЧТЕНИЮ И ТОЧНОМУ ВЫПОЛНЕНИЮ ВСЕХ ИНСТРУКЦИЙ, СОДЕРЖАЩИХСЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ, МОЖЕТ ПРИВЕСТИ К ПОВРЕЖДЕНИЮ ИЗДЕЛИЙ, ТРАВМАМ (ПОЛЬЗОВАТЕЛЯ ИЛИ ИНЫХ ЛИЦ) И ПОВРЕЖДЕНИЮ ИМУЩЕСТВА И ПРИВЕДЕТ К ОТМЕНЕ ЛЮБЫХ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ, ПРИМЕНИМЫХ К ИЗДЕЛИЯМ.

КОМПАНИЯ ILLUMINA НЕ НЕСЕТ НИКАКОЙ ОТВЕТСТВЕННОСТИ, ВОЗНИКАЮЩЕЙ ВСЛЕДСТВИЕ НЕНАДЛЕЖАЩЕГО ИСПОЛЬЗОВАНИЯ ИЗДЕЛИЙ, ОПИСАННЫХ В НАСТОЯЩЕМ ДОКУМЕНТЕ (ВКЛЮЧАЯ ИХ ЧАСТИ ИЛИ ЧАСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ).

© Illumina, Inc., 2022. Все права защищены.

Все товарные знаки являются собственностью компании Illumina, Inc. или их соответствующих владельцев. Информация о конкретных товарных знаках приведена на сайте www.illumina.com/company/legal.html.