

Програмне виправлення версії 1.0 для LRM

illumina®

Покрокові інструкції

Вступ

Компанії Illumina® стало відомо про наявність вразливості в системі безпеки програми Local Run Manager, і вона випустила програмний патч для захисту від віддаленого неналежного використання такої вразливості.

Local Run Manager — це окрема програма та частина конфігурації за замовчуванням у таких системах:

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

* Використовувати для діагностики in vitro.

Цей посібник застосовується до перелічених вище приладів Illumina, а також до зовнішніх комп'ютерів, на яких встановлена автономна версія Local Run Manager.

Уразливість — це неавтентифіковане віддалене виконання команд (Remote Command Execution, RCE) рівня 10.0 — «Критично» — за шкалою оцінки вразливості (Common Vulnerability Scoring System, CVSS) до застосування заходів усунення ризиків CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N.

До перелічених вище приладів потрібні наведені нижче заходи зниження ризиків для захисту від можливості отримання несанкціонованим користувачем доступу до одного або кількох приладів і віддаленої атаки.

Якщо з якоїсь причини не вдається запустити інсталятор, зверніться до розділу додаткових заходів щодо усунення ризиків наприкінці цього документа або повідомте про це за електронною адресою techsupport@illumina.com для отримання подальшої допомоги.

Щоб дізнатися, як завантажити або запитати копію патча, див. розділ [Отримання оновлення Local Run Manager](#).

- **Патч до версії 1.0.0** — оновлює вебконфігурацію Local Run Manager і вимикає віддалений доступ до інформаційних служб Інтернету (IIS, Internet Information Services).

Отримання патча системи безпеки Local Run Manager

Є 4 (чотири) варіанти отримання патча системи безпеки Local Run Manager.

Варіант 1: безпосереднє завантаження на власний прилад

Найшвидший спосіб отримати оновлення безпеки Local Run Manager — завантажити його на прилад безпосередньо з вебсайту хостингу.

1. Завантажте інсталятор патча за посиланням, наданим через захищену електронну пошту, на свій прилад.
2. Перенесіть файл у папку C:\Illumina на приладі.
3. Дотримуйтеся вказівок, які містяться в пункті [Застосування патча безпеки для Local Run Manager на стор. 4](#).

Варіант 2: завантаження інсталятора патча на комп'ютер і перенесення його на прилад через USB-накопичувач / спільну папку

i | Якщо ви не можете завантажити патч системи безпеки на прилад, ми рекомендуємо завантажити його на окремий комп'ютер, а потім перенести на прилад.

Перед використанням перевірте цілісність USB-накопичувача у фахівців з безпеки. (Рекомендовано.)

1. Завантажте інсталятор патча за посиланням, наданим через захищену електронну пошту, на свій комп'ютер або ноутбук.
2. Скопіюйте завантажений інсталятор патча на USB-накопичувач або спільну папку з комп'ютера.
3. Підключіть USB-накопичувач до приладу.
4. Скопіюйте інсталятор патча з USB-накопичувача або спільної папки в папку C:\Illumina на приладі.
5. Дотримуйтеся вказівок, які містяться в пункті [Застосування патча безпеки для Local Run Manager на стор. 4](#).

Варіант 3: запит технічної підтримки

Представник технічної підтримки компанії Illumina проведе вас через процес встановлення патча за допомогою одного з указаних далі методів.

- Технічна підтримка за допомогою віддаленої авторизації.
Представник технічної підтримки дистанційно підключиться до аналізатора та встановить патч від імені замовника.

i | До системи потрібно забезпечити віддалений доступ. Якщо у вас виникли запитання, зверніться по допомогу до представника місцевого IT-відділу.

Покрокові інструкції щодо програмного виправлення версії 1.0 для LRM

- Покрокові інструкції

Представник технічної підтримки надасть інструкції телефоном. Зверніться по допомогу до місцевого представника технічної підтримки.

Варіант 4: Замовлення накопичувача з попередньо налаштованою конфігурацією в Illumina

Захищені від запису USB-накопичувачі можуть бути замовлені клієнтом безкоштовно. Щоб замовити накопичувач зі встановленим патчем, зв'яжіться з нами за адресою techsupport@illumina.com.

i | На своєчасність доставки можуть вплинути затримки з надсиланням або відсутність запасів. Щоб захистити системи швидше, наполегливо рекомендується застосовувати метод, який уможливіть найбільш ефективний шлях усунення проблеми.

Застосування інсталеатора патча безпеки версії 1.0 Local Run Manager

Після запуску інсталеатор Illumina MSI (Microsoft Installer) оновить конфігурацію вебсервера Local Run Manager, щоб запобігти виконанню будь-якого вмісту, завантаженого користувачем, і заблокувати віддалений доступ до вебінтерфейсу Local Run Manager із мережевих з'єднань LAN.

i | Для тих користувачів, які використовують вебінтерфейс Local Run Manager для віддаленого доступу до приладів, цей робочий процес перестане функціонувати після встановлення цього оновлення. Компанія Illumina має намір відновити цю функціональність за допомогою постійного програмного виправлення цієї проблеми пізніше. Якщо це спричинить переривання налаштованих робочих процесів, зв'яжіться з techsupport@illumina.com для отримання подальшої допомоги.

Інсталеатор MSI застосовується до всіх версій Local Run Manager і автоматично визначає правильне виправлення на основі версії Local Run Manager, встановленої на приладі / комп'ютері.

Цей інсталеатор MSI також створює файл аудиту, який показує, що цей захід усунення ризиків було реалізовано разом із міткою часу, що відображає належне встановлення.

Запуск інсталеатора MSI: під час першого запуску інсталеатор MSI встановлює патч у систему та створює файл аудиту з указаним часом завершення.

i | Повторний запуск інсталеатора MSI надає доступ до функції **Repair** (Налагодження): користувач має можливість повторно застосувати або скасувати встановлення патча. Примітка. Скасування встановлення патча призведе до незахищеної конфігурації приладу.

Застосування патча безпеки для Local Run Manager

Щоб встановити патч, виконайте наступні кроки.

1. Увійдіть у систему з обліковим записом адміністратора (наприклад, sbsadmin).

i | Компанія Illumina рекомендує застосовувати патч тоді, коли прилад не працює. Якщо прилад працює, патч повинен застосовуватися негайно після завершення його роботи.

2. Знайдіть патч, що було завантажено в систему.
3. Перенесіть інстальатор патча в папку C:\Illumina (виняток з політики обмеженого використання програмного забезпечення).
4. Двічі клацніть значок інстальатора, щоб запустити інтерфейс.
5. Коли програма завантажиться, виберіть **Next (Далі)**, щоб розпочати встановлення патча.
6. На екрані Installation Completion (Завершення встановлення) виберіть **Finish (Готово)**.

i | У випадку, якщо потрібна верифікація звіту про встановлення, див. розділ [Верифікація на стор. 5](#).

i | Після завершення встановлення потрібне перезавантаження.

Налагодження

У разі помилки замовник може виконати налагодження встановлення, дотримуючись наведених нижче інструкцій.

1. Увійдіть у систему з обліковим записом адміністратора (наприклад, sbsadmin).
2. Знайдіть патч, що було завантажено в систему.
3. Перенесіть інстальатор патча в папку C:\Illumina (виняток з політики обмеженого використання програмного забезпечення).
4. Двічі клацніть значок інстальатора, щоб запустити інтерфейс.
5. Інстальатор автоматично визначить, чи запускався інструмент конфігурації раніше, і надасть доступ до нових функцій.
 - a. Change (Зміна): виділене сірим кольором і недоступне.
 - b. Repair (Налагодження): виправлення помилок та варіанти зміни конфігурації.
 - c. Remove (Видалення): видалення патча та скидання до конфігурації за замовчуванням (див. [Скасування встановлення на стор. 5](#)).
6. На екрані Installation Completion (Завершення встановлення) виберіть **Finish (Готово)**.

i | У випадку, якщо потрібна верифікація звіту про встановлення, див. розділ [Верифікація на стор. 5](#).

Покрокові інструкції щодо програмного виправлення версії 1.0 для LRM

i | Після завершення встановлення потрібне перезавантаження.

Скасування встановлення

Скасування встановлення патча відкликає зміни, внесені до файлу конфігурації хоста програми.

1. Увійдіть в систему через обліковий запис адміністратора (наприклад, sbsadmin).
2. Знайдіть патч, що було завантажено в систему.
3. Перенесіть інстальатор патча в папку C:\Illumina (виняток з політики обмеженого використання програмного забезпечення).
4. Двічі клацніть значок інстальатора, щоб запустити інтерфейс.
5. Виберіть **Remove** (Видалити), щоб скасувати встановлення патча та скинути всі значення до налаштувань за замовчуванням.
6. Виберіть **Remove** (Видалити), щоб перевірити опцію скасування встановлення патча та скинути всі значення до налаштувань за замовчуванням.

! | Через це налаштування система стане незахищеною та підлягатиме ризику атаки. Перед прийняттям рішення про скасування патча наполегливо рекомендується усунути будь-які технічні причини, які спонукали розгляд видалення патча.

7. На екрані Installation Completion (Завершення встановлення) виберіть **Finish** (Готово).

i | У випадку, якщо потрібна верифікація звіту про встановлення, див. розділ [Верифікація на стор. 5](#).

i | У кінці встановлення рекомендується провести перезавантаження.

Верифікація

Якщо потрібно верифікувати встановлення, буде створено файл верифікації, який містить позначку дати та часу, версію встановленої програми Local Run Manager та інші ключові значення перевірки. Щоб отримати цей файл, зв'яжіться з techsupport@illumina.com.

Додаткові рекомендації щодо заходів усунення ризиків і безпеки


Безпечне встановлення приладів, призначених лише для досліджень (RUO), і медичних пристроїв для діагностики залежить від рівнів захисту. Компанія Illumina наполегливо рекомендує встановлювати прилади й пристрої в найменшій підмережі або безпечному середовищі з надійними пристроями. Доцільним є використання брандмауерів та інших політик мережі для обмеження іншого вхідного та вихідного доступу.

Ми також рекомендуємо вжити вказаних далі заходів.

- Увімкнути захист на транспортному рівні (Transport Layer Security, TLS), щоб переконатися, що весь зв'язок поза приладом зашифровано.
 - Щоб увімкнути захист TLS, див. посібник з програмного забезпечення Local Run Manager.

Альтернативні варіанти

Якщо з якоїсь причини виконати оновлення неможливо, зменшити ризик допоможуть наведені нижче заходи, які можна виконати вручну.

- Вимкніть віддалений доступ до Local Run Manager, додавши правила брандмауера Windows, щоб блокувати вхідні з'єднання через порт 80 і 443.
Інстальатор MSI автоматично блокує віддалені вхідні з'єднання в конфігурації вебсервера Local Run Manager. Ручний захід усунення ризиків, який досягає того ж результату, полягає в застосуванні конфігурації брандмауера Windows з метою блокування вхідних з'єднань до з'єднань HTTP (TCP:80) і HTTPS (TLS, TCP:443).
Доступ до Local Run Manager після впровадження можна отримати лише на комп'ютері, на якому встановлено Local Run Manager. Програма більше не буде доступна з інших комп'ютерів, підключених до тієї ж мережі.
-  Якщо робочий процес користувача передбачає віддалений доступ до Local Run Manager, ця функція більше не працюватиме.
- Зведіть до мінімуму кількість інших мережевих пристроїв.
Створення такої конфігурації мережі, у якій буде зведено до мінімуму кількість мережевих пристроїв, які обмінюються даними з ураженим приладом, зменшить можливість неналежного використання. Чим менше підключень доступно для системи, тим менше можливостей доступу.
Для цього може знадобитися консультація з місцевим відділом інформаційної безпеки або спеціалістами IT-відділу.
- Видаліть прилад з мережі.
Якщо інші варіанти є практично нездійсненними, остаточним засобом зниження ризику є повне видалення приладу з мережі. Слід зауважити, що це вимкне доступ до сервісів Illumina Cloud/SaaS, таких як Proactive і BaseSpace® Sequence Hub, а також типових робочих процесів передачі геномних даних.
Для цього може знадобитися консультація з місцевим відділом інформаційної безпеки або спеціалістами IT-відділу.

Розслідування ймовірного несанкціонованого доступу.

Наведені далі кроки можуть допомогти оператору приладу визначити, чи мав місце доступ несанкціонованого користувача в систему.

1. Перевірте журнали інформаційного інтернет-сервера, що зберігаються за адресою C:\inetpub\logs\LogFiles\W3SVC1, на наявність неналежних викликів.

- Звичайні виклики на вебсервер Local Run Manager виглядають так:

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

- Неналежні виклики на вебсервер Local Run Manager можуть виглядати, наприклад, так:

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

2. Перевірте журнали інформаційного інтернет-сервера на ознаки завантаження методом POST контенту, що не є файлами маніфесту. Наприклад, такі виклики можуть указувати на підозрілу активність:

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

3. Якщо встановлено програму-антивірус, перевірте файли журналів на наявність ознак ненормального поведження.
4. Перевірте журнали Windows на ознаки ненормальних повідомлень про помилки.
Якщо зловмисник отримав доступ до прав адміністратора, він мав можливість змінити або видалити всі локальні журнали та події приладу.

Перевірте всі кінцеві точки, через які система може намагатися отримати доступ. Список очікуваних зовнішніх підключень див. у [брандмауері керівного комп'ютера](#).

За потреби зверніться по допомогу до служби технічної підтримки Illumina.

Історія редакцій

Документ	Дата	Опис зміни
Документ № 200017330 v02	Квітень 2022 р.	Додано рекомендацію щодо застосування патча тоді, коли прилад не працює. Додано вказівку про потребу перезавантаження приладу після встановлення патча. Виправлено історію редакцій для версії v01.
Документ № 200017330, версія 01	Квітень 2022 р.	Назву документа змінено на «Покрокові інструкції щодо програмного виправлення версії 1.0 для LRM». Видалено всі згадування версії 1.0.1. Додано розділ, який описує розслідування ймовірного несанкціонованого доступу.
Документ № 200017330, версія 00	Березень 2022 р.	Початкова редакція.

Цей документ і його зміст є власністю компанії Illumina, Inc. і її філій (надалі — Illumina). Він призначений лише для того, щоб користувач використовував вироби тільки за угодою в цілях, описаних у цьому документі. Цей документ і його зміст не слід використовувати або поширювати з будь-якою іншою метою та/або для іншого обговорення, розкриття або відтворення тим або іншим чином без попередньої письмової згоди компанії Illumina. Цим документом компанія Illumina не надає жодного дозволу на свій патент, товарний знак, авторське право або загальноприйняті права, а також на подібні права будь-яких третіх сторін.

Щоб гарантувати правильне та безпечне використання виробів, описаних у цьому документі, кваліфікований і належно навчений персонал повинен суворо та чітко дотримуватись інструкцій, описаних у цьому документі. Перед використанням цих виробів потрібно повністю прочитати й зрозуміти весь зміст цього документа.

НЕПОВНЕ ВИВЧЕННЯ ВСІХ ЗАЗНАЧЕНИХ У ЦЬОМУ ДОКУМЕНТІ ВКАЗІВОК І НЕЧІТКЕ ДОТРИМАННЯ МОЖЕ ПРИЗВОДИТИ ДО ПОШКОДЖЕННЯ ЦИХ ВИРОБІВ, ТРАВМУВАННЯ ЛЮДЕЙ, ВКЛЮЧНО З КОРИСТУВАЧАМИ АБО ІНШИМИ ОСОБАМИ, І ПОШКОДЖЕННЯ ІНШОЇ ВЛАСНОСТІ, А ТАКОЖ ПРИЗВЕДЕ ДО ВТРАТИ БУДЬ-ЯКИХ ГАРАНТІЙНИХ ЗОБОВ'ЯЗАНЬ, ЗАСТОСОВНИХ ДО ЦИХ ВИРОБІВ.

КОМПАНІЯ ILLUMINA НЕ НЕСЕ ЖОДНОЇ ВІДПОВІДАЛЬНОСТІ, ЩО ВИНИКАЄ ВНАСЛІДОК НЕНАЛЕЖНОГО ВИКОРИСТАННЯ ВИРОБІВ, ОПИСАНИХ У ЦЬОМУ ДОКУМЕНТІ (ВКЛЮЧНО З ЙОГО ЧАСТИНАМИ АБО ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ).

© Illumina, Inc., 2022. Усі права застережено.

Усі товарні знаки — власність компанії Illumina, Inc. або їхніх відповідних власників. Конкретна інформація про товарні знаки зазначена на сторінці www.illumina.com/company/legal.html.