

Poprawka oprogramowania LRM, illumina® wer. 1.0

Instrukcja obsługi

Wstęp

Firma Illumina® została ostrzeżona o luce w zabezpieczeniach występującej w oprogramowaniu Lokalnego menedżera przebiegu i dostarczyła poprawkę do oprogramowania, która chroni przed zdalnym wykorzystaniem tej luki.

Lokalny menedżer przebiegu jest aplikacją autonomiczną i elementem konfiguracji domyślnej następujących systemów:

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

*Do stosowania w diagnostyce „in vitro”

Ten przewodnik dotyczy instrumentów Illumina wymienionych powyżej, a także komputerów poza aparatem, na których zainstalowano samodzielną wersję programu Lokalnego menedżera przebiegu.

Luka w zabezpieczeniach umożliwia nieuprawnione zdalne wykonanie kodu (RCE, Remote Command Execution) i uzyskała wynik 10.0 Critical (Krytyczny) w systemie CVSS:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

Aby zabezpieczyć się przed możliwością uzyskania przez nieupoważnionego użytkownika dostępu do jednego lub więcej aparatów i przeprowadzenia zdalnego ataku, na wymienionych powyżej urządzeniach należy wykonać następujące czynności łagodzące.

Jeśli z jakiegoś powodu nie można uruchomić instalatora, należy zapoznać się z sekcją dotyczącą dodatkowych środków bezpieczeństwa na końcu tego dokumentu lub skontaktować się z działem pomocy technicznej (techsupport@illumina.com) w celu uzyskania dodatkowej pomocy.

Informacje o możliwościach pobrania poprawki lub uzyskania jej kopii zawiera sekcja [Uzyskiwanie aktualizacji oprogramowania Lokalnego menedżera przebiegu](#).

- **Poprawka v1.0.0** – zaktualizuje konfigurację internetową oprogramowania Lokalny menedżer przebiegu i wyłączy dostęp zdalny do internetowych usług informacyjnych (IIS, Internet Information Services).

Uzyskaj poprawkę bezpieczeństwa Lokalnego menedżera przebiegu

Istnieją cztery (4) opcje uzyskania poprawki zabezpieczającej Lokalnego menedżera przebiegu.

Opcja 1 - Pobranie bezpośrednio na aparat

Najszybszym sposobem uzyskania aktualizacji zabezpieczeń oprogramowania Lokalny menedżer przebiegu jest pobranie jej z witryny internetowej bezpośrednio na aparat.

1. Pobrać instalator poprawki na aparat przy użyciu łącza przesłanego przez bezpieczną pocztę e-mail.
2. Przenieść plik do folderu C:\Illumina aparatu.
3. Postępuj zgodnie z instrukcjami w sekcji [Zastosowanie poprawki zabezpieczeń oprogramowania Lokalny menedżer przebiegu na stronie 4](#).

Opcja 2 - Pobranie instalatora poprawki na komputer i przeniesienie go do aparatu za pośrednictwem dysku USB / folderu udostępnionego

i | Jeśli nie możesz pobrać poprawki bezpieczeństwa do aparatu, zalecamy pobranie jej na osobny komputer, a następnie przesłanie jej do instrumentu.

Przed użyciem dysku USB należy potwierdzić jego integralność u przedstawiciela zespołu ds. bezpieczeństwa (zalecane).

1. Pobrać instalator poprawki na komputer lub laptop przy użyciu łącza przesłanego przez bezpieczną pocztę e-mail.
2. Skopiować pobrany instalator poprawki z komputera na dysk USB lub do folderu udostępnionego.
3. Dysk USB podłączyć do aparatu.
4. Skopiować instalator poprawki z dysku USB lub folderu udostępnionego do folderu C:\Illumina aparatu.
5. Postępuj zgodnie z instrukcjami w sekcji [Zastosowanie poprawki zabezpieczeń oprogramowania Lokalny menedżer przebiegu na stronie 4](#).

Opcja 3 - Poproś o pomoc techniczną

Przedstawiciel działu pomocy technicznej firmy Illumina przeprowadzi Cię przez proces instalowania poprawki przy użyciu jednej z następujących metod:

- Logowanie zdalne przedstawiciela działu pomocy technicznej
Przedstawiciel działu pomocy technicznej zaloguje się zdalnie do analizatora i zainstaluje poprawkę w imieniu klienta.

i | System musi być dostępny zdalnie. W przypadku pytań należy się zwrócić o pomoc do przedstawiciela lokalnego zespołu IT.

- Instruktaż przez telefon

Przedstawiciel działu pomocy technicznej udzieli instruktażu przez telefon. W celu uzyskania pomocy należy się skontaktować z lokalnym przedstawicielem działu pomocy technicznej.

Opcja 4 - Zamówienie fabrycznie skonfigurowanego dysku w firmie Illumina

Klient może bezpłatnie zamówić zabezpieczone przed zapisem dyski USB. Aby zamówić dysk z zainstalowaną poprawką, prosimy o kontakt pod adresem techsupport@illumina.com.

- i** | Mogą wystąpić opóźnienia w wysyłce, a na terminowość dostawy może wpłynąć stan zapasów. Aby niezwłocznie chronić systemy, zdecydowanie zaleca się wybór metody, która zapewni najskuteczniejsze rozwiązanie problemu.

Zastosuj instalator Lokalnego menedżera przebiegu Security Patch v.1.0

Illumina MSI (Instalatora Microsoft), po uruchomieniu, zaktualizuje konfigurację serwera sieciowego Lokalnego menedżera przebiegu, aby zapobiec wykonywaniu treści przesłanych przez użytkownika i zablokować wszelki zdalny dostęp do interfejsu sieciowego Lokalnego menedżera przebiegu z połączeń sieciowych LAN.

- i** | Po zainstalowaniu poprawki użytkownicy utracą możliwość uzyskiwania dostępu zdalnego do aparatów przy użyciu interfejsu internetowego Lokalnego menedżera przebiegu. Firma Illumina zamierza przywrócić taką funkcję później przez trwałe rozwiązanie tego problemu w oprogramowaniu. Jeśli brak dostępu zdalnego spowoduje zakłócenie ustalonych procedur, prosimy o kontakt w celu uzyskania dalszej pomocy: techsupport@illumina.com.

Instalator MSI ma zastosowanie do wszystkich wersji oprogramowania Lokalny menedżer przebiegu i automatycznie określi odpowiednią poprawkę na podstawie wersji oprogramowania zainstalowanej na aparacie/komputerze.

Instalator MSI utworzy też plik kontrolny zawierający informację o wdrożeniu tego środka zmniejszającego ryzyko oraz znacznik czasu potwierdzający właściwą instalację.

Uruchamianie instalatora MSI – podczas pierwszego uruchomienia instalator MSI zastosuje poprawkę w systemie i utworzy plik kontrolny ze znacznikiem czasu ukończenia.

- i** | Podczas ponownego uruchomienia instalatora MSI będzie dostępna opcja **Repair** (Naprawa), która umożliwi użytkownikowi ponowne zastosowanie poprawki lub jej wycofanie. Uwaga: Cofnięcie poprawki spowoduje niezabezpieczoną konfigurację aparatu.

Zastosowanie poprawki zabezpieczeń oprogramowania Lokalny menedżer przebiegu

Aby zainstalować poprawkę:

1. Zalogować się do systemu przy użyciu konta administratora (np. sbsadmin).
 - i** | Illumina zaleca instalowanie poprawki, gdy aparat nie jest uruchomiony. Jeśli aparat wykonuje cykl, poprawkę należy zastosować natychmiast po zakończeniu cyklu.
2. Znaleźć poprawkę pobraną do systemu.
3. Przenieść instalator poprawki do folderu C:\Illumina (wykluczyć z zasad ograniczeń oprogramowania).
4. Kliknąć dwukrotnie ikonę instalatora, aby uruchomić interfejs.
5. Po załadowaniu aplikacji wybrać **Next** (Dalej), aby rozpocząć instalację poprawki.
6. Na ekranie „Installation Completion” (Zakończenie instalacji) wybrać **Finish** (Zakończ).

i | Jeśli jest wymagany raport weryfikacji instalacji, należy się zapoznać z sekcją [Weryfikacja na stronie 5](#).

i | Wymagane jest ponowne uruchomienie systemu po zakończeniu instalacji.

Naprawa

W przypadku wystąpienia błędu klient może wykonać procedurę naprawy, postępując zgodnie z poniższą instrukcją:

1. Zalogować się do systemu przy użyciu konta administratora (np. sbsadmin).
2. Znaleźć poprawkę pobraną do systemu.
3. Przenieść instalator poprawki do folderu C:\Illumina (wykluczyć z zasad ograniczeń oprogramowania).
4. Kliknąć dwukrotnie ikonę instalatora, aby uruchomić interfejs.
5. Instalator automatycznie wykryje, czy wcześniej zostało uruchomione narzędzie konfiguracji, i przedstawi nowe opcje:
 - a. „Change” (Zmień): wyszarzona i niedostępna.
 - b. „Repair” (Napraw): naprawia błędy i umożliwia ponowną konfigurację.
 - c. „Remove” (Usuń): odinstalowuje poprawkę i przywraca konfigurację domyślną (patrz: [Odinstalowanie na stronie 5](#)).
6. Na ekranie „Installation Completion” (Zakończenie instalacji) wybrać **Finish** (Zakończ).

i | Jeśli jest wymagany raport weryfikacji instalacji, należy się zapoznać z sekcją [Weryfikacja na stronie 5](#).

i | Wymagane jest ponowne uruchomienie systemu po zakończeniu instalacji.

Odinstalowanie

Odinstalowanie poprawki wycofuje modyfikacje wprowadzone w pliku konfiguracji hosta aplikacji.

1. Zalogować się do systemu przy użyciu konta administratora (np. sbsadmin).
2. Znaleźć poprawkę pobraną do systemu.
3. Przenieść instalator poprawki do folderu `C:\Illumina` (wykluczyć z zasad ograniczeń oprogramowania).
4. Kliknąć dwukrotnie ikonę instalatora, aby uruchomić interfejs.
5. Wybrać **Remove** (Usuń), aby odinstalować poprawkę i przywrócić wszystkie wartości do ustawień domyślnych.
6. Wybrać **Remove** (Usuń), aby sprawdzić możliwość odinstalowania poprawki i przywrócenia wszystkich wartości do ustawień domyślnych.

! | To ustawienie spowoduje, że system będzie niezabezpieczony i narażony na atak. Zdecydowanie zaleca się, aby przed wybraniem opcji odinstalowania ocenić konsekwencje techniczne usunięcia poprawki.

7. Na ekranie „Installation Completion” (Zakończenie instalacji) wybrać **Finish** (Zakończ).

i | Jeśli jest wymagany raport weryfikacji instalacji, należy się zapoznać z sekcją [Weryfikacja na stronie 5](#).

i | Zalecane jest ponowne uruchomienie systemu po zakończeniu instalacji.

Weryfikacja

Jeśli jest konieczna weryfikacja instalacji, zostanie wygenerowany plik weryfikacji, który zawiera znacznik daty i godziny, wersję zainstalowanego oprogramowania Lokalny menedżer przebiegu oraz inne ważne wartości weryfikacyjne. W celu uzyskania tego pliku prosimy o kontakt pod adresem techsupport@illumina.com.

Dodatkowe środki bezpieczeństwa i zalecenia dotyczące zabezpieczeń


Bezpieczne wdrażanie instrumentów RUO i urządzeń medycznych Dx zależy od poziomów zabezpieczeń. Firma Illumina zdecydowanie zaleca wdrażanie aparatów i wyrobów w najmniejszych podsięciach lub w kontekście zabezpieczeń z zaufanymi urządzeniami. Bardzo wskazane jest zastosowanie zapór lub innych zasad sieciowych, aby ograniczyć ruch przychodzący i wychodzący.

Ponadto rekomendujemy:

- Włączenie protokołu TLS (TLS, Transport Layer Security) w celu zapewnienia szyfrowania całej komunikacji poza aparatem.
 - Aby włączyć protokół TLS (TLS, Transport Layer Security), należy się zapoznać z „Instrukcją obsługi oprogramowania Lokalny menedżer przebiegu”.

Alternatywne możliwości

Jeśli z jakiegoś powodu nie można zastosować poprawki, zagrożenie zmniejszą następujące działania zaradcze:

- Wyłączenie dostępu zdalnego do Lokalnego menedżera przebiegu przez dodanie reguł zapory systemu Windows, które zablokują połączenia przychodzące na porcie 80 i 443.
Instalator MSI automatycznie zablokuje zdalne połączenia przychodzące w konfiguracji serwera internetowego Lokalnego menedżera przebiegu. Takie same efekty ograniczające ryzyko zapewnia wdrożenie konfiguracji zapory systemu Windows, która zablokuje połączenia przychodzące na porcie HTTP (TCP:80) oraz porcie HTTPS (TLS, TCP:443).
Po zastosowaniu takich środków zaradczych oprogramowanie Lokalny menedżer przebiegu będzie dostępne tylko na komputerze, na którym je zainstalowano. Nie będzie już dostępne z innych komputerów podłączonych do tej samej sieci.
-  Jeśli procedura użytkownika wymaga zdalnego dostępu do Lokalnego menedżera przebiegu, taka funkcja nie będzie działać.
- Zmniejszenie liczby innych urządzeń sieciowych.
Skonfigurowanie sieci w celu zmniejszenia liczby urządzeń sieciowych, które mogą łączyć się z zagrożonym aparatem, ograniczy możliwość przeniesienia zagrożenia. Im mniej połączeń skonfigurowanych w systemie, tym mniej możliwości uzyskania do niego dostępu.
Zastosowanie takich środków zmniejszających ryzyko może wymagać konsultacji z lokalnym zespołem ds. bezpieczeństwa informacji lub IT.
- Usunięcie aparatu z sieci.
Jeśli żadna inna opcja nie jest możliwa, ostatecznym środkiem zaradczym jest całkowite usunięcie aparatu z sieci. Spowoduje to wyłączenie dostępu do usług w chmurze / usług SaaS firmy Illumina, takich jak Proactive i BaseSpace® Sequence Hub, a także typowych procedur obejmujących przenoszenie danych genomicznych.
Zastosowanie takich środków zmniejszających ryzyko może wymagać konsultacji z lokalnym zespołem ds. bezpieczeństwa informacji lub IT.

Badanie potencjalnego nieautoryzowanego dostępu.

Poniższe kroki mogą pomóc operatorowi aparatu w ustaleniu, czy nieautoryzowany użytkownik uzyskał dostęp do systemu:

Poprawka oprogramowania LRM, wersja 1.0 — instrukcja obsługi

1. Przeanalizować dzienniki IIS przechowywane w katalogu C:\inetpub\logs\LogFiles\W3SVC1 pod kątem nietypowych poleceń.

- Normalne polecenia przesyłane do serwera sieciowego narzędzia Lokalny menedżer przebiegu są wyświetlane następująco:

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

- Nietypowe polecenia przesyłane do serwera sieciowego narzędzia Lokalny menedżer przebiegu mogą wyglądać jak w następujących przykładach:

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

2. Przeanalizować dziennik IIS pod kątem śladów poleceń POST dotyczących zawartości innej niż pliki wykazu. Przykładowo następujące polecenia mogą wskazywać na podejrzane działania:

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

3. Jeśli zainstalowana jest aplikacja antywirusowa lub chroniąca przed złośliwym oprogramowaniem, należy sprawdzić dzienniki oprogramowania pod kątem oznak nietypowego zachowania.
4. Sprawdzić dzienniki systemu Windows pod kątem oznak nietypowych komunikatów o błędach. Jeśli osoba stwarzająca zagrożenie uzyska dostęp z prawami administratora, będzie mogła zmieniać lub usuwać wszystkie lokalne dzienniki i zdarzenia aparatów.

Sprawdź, czy nie ma punktów końcowych, do których system mógł próbować uzyskać dostęp. Listę normalnych połączeń wychodzących można znaleźć w sekcji [Zapora komputera sterującego](#).

W razie potrzeby należy skontaktować się z działem pomocy technicznej firmy Illumina, aby uzyskać pomoc.

Historia wersji

Dokument	Data	Opis zmiany
Nr dokumentu 200017330 wer. 02	Kwiecień 2022 r.	Dodano zalecenie zastosowania poprawki, gdy aparat nie jest uruchomiony. Dodano instrukcję, że po instalacji poprawki wymagane jest ponowne uruchomienie aparatu. Poprawiono opis historii zmian w wersji 01.
Nr dokumentu 200017330 wer. 01	Kwiecień 2022 r.	Zmieniono tytuł dokumentu na „Poprawka oprogramowania LRM, wersja 1.0 — instrukcja obsługi”. Usunięto wszelkie wzmianki o wersji 1.0.1. Dodano sekcję obejmującą badanie potencjalnego nieautoryzowanego dostępu.
Nr dokumentu 200017330 wer. 00	Marzec 2022 r.	Pierwsze wydanie.

Niniejszy dokument oraz jego treść stanowią własność firmy Illumina, Inc. oraz jej podmiotów zależnych („Illumina”) i są przeznaczone wyłącznie do użytku zgodnego z umową przez klienta firmy w związku z użytkowaniem produktów opisanych w niniejszym dokumencie, z wyłączeniem innych celów. Niniejszy dokument oraz jego treść nie będą wykorzystywane ani rozpowszechniane do innych celów i/lub publikowane w inny sposób, ujawniane ani kopiowane bez pisemnej zgody firmy Illumina. Firma Illumina na podstawie niniejszego dokumentu nie przenosi żadnych licencji podlegających przepisom w zakresie patentów, znaków towarowych czy praw autorskich ani prawu powszechnemu lub prawom pokrewnym osób trzecich.

W celu zapewnienia właściwego i bezpiecznego użytkowania produktów opisanych w niniejszym dokumencie podane instrukcje powinny być ściśle przestrzegane przez wykwalifikowany i właściwie przeszkolony personel. Przed rozpoczęciem użytkowania tych produktów należy zapoznać się z całą treścią niniejszego dokumentu.

NIEZAPOZNANIE SIĘ LUB NIEDOKŁADNE PRZESTRZEGANIE WSZYSTKICH INSTRUKCJI PODANYCH W NINIEJSZYM DOKUMENCIE MOŻE SPOWODOWAĆ USZKODZENIE PRODUKTÓW LUB OBRAŻENIA CIAŁA UŻYTKOWNIKÓW LUB INNYCH OSÓB ORAZ USZKODZENIE INNEGO MIENIA, A TAKŻE SPOWODUJE UNIEWAŻNIENIE WSZELKICH GWARANCJI DOTYCZĄCYCH PRODUKTÓW.

FIRMA ILLUMINA NIE PONOSI ODPOWIEDZIALNOŚCI ZA NIEWŁAŚCIWE UŻYTKOWANIE PRODUKTÓW (W TYM ICH CZĘŚCI I OPROGRAMOWANIA) OPISANYCH W NINIEJSZYM DOKUMENCIE.

© 2022 Illumina, Inc. Wszelkie prawa zastrzeżone.

Wszystkie znaki towarowe są własnością firmy Illumina, Inc. lub ich odpowiednich właścicieli. Szczegółowe informacje na temat znaków towarowych można znaleźć na stronie www.illumina.com/company/legal.html.