

LRM-programvareoppdatering 1.0 illumina®

Veiledning

Innledning

illumina® har blitt oppmerksom på et sikkerhetsproblem i Local Run Manager-programvaren og har levert en programvareoppdatering for å beskytte mot ekstern utnyttelse av dette sikkerhetsproblemet.

Local Run Manager er en frittstående programvare og del av standardkonfigurasjonen på følgende systemer:

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

*Til in vitro-diagnostisk bruk.

Denne veiledningen gjelder illumina-instrumentene som er oppført ovenfor, og også for datamaskiner utenfor instrumentet hvor den frittstående versjonen av Local Run Manager er installert.

Problemet er en Unauthenticated Remote Command Execution (RCE) (uautentisert kjøring av ekstern kommando) som dersom den ikke utbedres har en CVSS-rangering på 10.0 Critical (kritisk),

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

De følgende trinnene for problembegrensning er nødvendige på instrumentene oppført ovenfor, for å beskytte mot muligheten for at en uautorisert bruker får tilgang til ett eller flere instrumenter og utfører et angrep via ekstern tilgang.

Dersom det av en eller annen grunn ikke er mulig å kjøre installasjonsprogrammet, ber vi deg lese avsnittet om ytterligere problembegrensningsmetoder nederst i dette dokumentet eller ta kontakt med techsupport@illumina.com for ytterligere hjelp.

Se [Hente oppdateringen for Local Run Manager](#) for alternativer for hvordan du laster ned eller ber om en kopi av oppdateringen.

- **v1.0.0-oppdateringen** – oppdaterer nettkonfigurasjonen for Local Run Manager og deaktiverer tilgang til Internet Information Services (IIS) (Internett-informasjontjenester).

Hente sikkerhetsoppdateringen for Local Run Manager

Det er fire (4) alternativer for å hente sikkerhetsoppdateringen for Local Run Manager.

Alternativ 1 — Last ned direkte til instrumentet

Den raskeste måten å hente sikkerhetsoppdateringen for Local Run Manager på er å laste den ned rett fra instrumentets nettsted.

1. Last ned installasjonsprogrammet for oppdateringen fra lenken du har fått oppgitt via sikker e-post til instrumentet.
2. Overfør filen til mappen C:\Illumina på instrumentet.
3. Følg instruksjonene i [Ta i bruk sikkerhetsoppdateringen for Local Run Manager på side 4](#).

Alternativ 2 — Last ned installasjonsprogrammet for oppdateringen til datamaskinen og overfør det til instrumentet via USB-stasjon / delt mappe

i | Hvis du ikke kan laste ned sikkerhetsoppdateringen til instrumentet, anbefaler vi at du laster den ned til en egen datamaskin og deretter overfører den til instrumentet.

Få det bekreftet av sikkerhetspersonellet at USB-stasjonen fungerer før du bruker den. (Anbefalt)

1. Last ned installasjonsprogrammet for oppdateringen fra lenken du har fått oppgitt via sikker e-post til den stasjonære eller bærbare datamaskinen.
2. Kopier det nedlastede installeringsprogrammet til USB-stasjonen eller en delt mappe på datamaskinen.
3. Dersom du bruker en USB-stasjon, stikker du stasjonen inn i instrumentet.
4. Kopier installasjonsprogrammet fra USB-stasjonen eller den delte mappen til mappen C:\Illumina på instrumentet.
5. Følg instruksjonene i [Ta i bruk sikkerhetsoppdateringen for Local Run Manager på side 4](#).

Alternativ 3 — Be om teknisk støtte

En representant for Illumina teknisk støtte vil veilede deg gjennom oppdateringsprosessen ved hjelp av en av følgende metoder:

- Ekstern innlogging for teknisk støtte
En representant for teknisk støtte vil få ekstern tilgang til analysatoren og installere oppdateringen på vegne av kunden.

i | Systemet må være tilgjengelig for eksterne tilkoblinger. Ta kontakt med den lokale IT-representanten dersom du har spørsmål.

- Veiledning

En representant for teknisk støtte gir veiledning via telefon. Kontakt den lokale representanten for teknisk støtte dersom du trenger hjelp.

Alternativ 4 — Bestille en forhåndskonfigurert stasjon fra Illumina

Kunden kan bestille en gratis skrivebeskyttet USB-stasjon. Ta kontakt med techsupport@illumina.com for å bestille stasjonen med oppdateringen installert.

i | Det kan være forsinkelser relatert til forsendelse eller inventar som kan påvirke tidspunktet for levering. Det anbefales å beskytte systemer så raskt som mulig ved å bruke metoden som gir den mest effektive løsningen.

Ta i bruk installasjonsprogrammet Local Run Manager Security Patch v.1.0

Illumina MSI (Microsoft Installer), når det kjøres, vil oppdatere nettserverkonfigurasjonen til Local Run Manager for å forhindre kjøring av brukeropplastet innhold og blokkere all ekstern tilgang til Local Run Managers nettgrensesnitt fra LAN-nettverksforbindelser.

i | For brukere som bruker Local Run Managers nettgrensesnitt til å få ekstern tilgang til instrumenter, vil denne arbeidsflyten ikke lenger fungere etter at denne oppdateringen er installert. Illumina planlegger å gjenopprette denne funksjonaliteten når dette problemet får en permanent løsning senere. Dersom dette medfører avbrudd i etablert arbeidsflyt, ber vi dere ta kontakt med techsupport@illumina.com for mer hjelp.

MSI-installasjonsprogrammet kan brukes til alle versjoner av Local Run Manager og vil automatisk bestemme riktig problemretting basert på hvilken versjon av Local Run Manager som er installert på instrumentet/datamaskinen.

Dette MSI-installasjonsprogrammet vil også opprette en revisjonsfil som viser at denne problembegrensningen er implementert samt et tidsstempel for å vise at korrekt installasjon er utført.

Kjøre MSI-installasjonsprogrammet – første gang MSI-installasjonsprogrammet kjøres vil installasjonsprogrammet oppdatere systemet og opprette en revisjonsfil med fullførelsestid.

i | Hvis MSI-installasjonsprogrammet kjøres igjen, vises alternativet **Repair** (Reparer), hvor brukeren får anledning til å installere oppdateringen på nytt eller rulle tilbake oppdateringen. Merk: Tilbakerulling av oppdateringen fører til en usikker instrumentkonfigurasjon.

Ta i bruk sikkerhetsoppdateringen for Local Run Manager

Slik installerer du oppdateringen:

1. Logg på systemet med en administratorkonto (f.eks. sbsadmin).

i | Illumina anbefaler at oppdateringen utføres når instrumentet ikke kjører. Hvis instrumentet utfører en kjøring, bør oppdateringen utføres umiddelbart etter at kjøringen er fullført.

2. Finn oppdateringen som ble lastet ned til systemet.
3. Flytt installasjonsprogrammet for oppdateringen til mappen C:\Illumina (unntatt fra programvarebegrensingspolicy).
4. Dobbeltklikk på installasjonsprogramikonet for å starte grensesnittet.
5. Når programmet laster inn, velger du **Next** (Neste) for å begynne installasjonen av oppdateringen.
6. Velg **Finish** (Fullfør) i skjermbildet Installation Completion (Fullfør installasjon).

i | Dersom det kreves verifisering av installasjonsrapport, se [Verifisering på side 5](#).

i | Det er nødvendig å starte på nytt når installasjonen er fullført.

Reparasjon

Dersom det oppstår en feil, kan kunden utføre reparasjon av installasjonen ved å følge instruksjonene nedenfor:

1. Logg på systemet med en administratorkonto (f.eks. sbsadmin).
2. Finn oppdateringen som ble lastet ned til systemet.
3. Flytt installasjonsprogrammet for oppdateringen til mappen C:\Illumina (unntatt fra programvarebegrensingspolicy).
4. Dobbeltklikk på installasjonsprogramikonet for å starte grensesnittet.
5. Installasjonsprogrammet oppdaterer automatisk om konfigurasjonsverktøyet har blitt startet tidligere, og gir nye alternativer:
 - a. Change (Endre): Nedtonet og ikke tilgjengelig
 - b. Repair (Reparer): Reparerer feil og gir alternativer for omkonfigurasjon.
 - c. Remove (Fjern): Avinstallerer oppdateringen og tilbakestillers til standardkonfigurasjon (se [Avinstallasjon på side 5](#))
6. Velg **Finish** (Fullfør) i skjermbildet Installation Completion (Fullfør installasjon).


i | Dersom det kreves verifisering av installasjonsrapport, se [Verifisering på side 5](#).

i | Det er nødvendig å starte på nytt når installasjonen er fullført.

Avinstallasjon


Avinstallasjon av oppdateringen tilbakestiller endringene som er gjort i vertskonfigurasjonsfilen for programmet.

1. Logg på systemet med en administratorkonto (f.eks. sbsadmin).
2. Finn oppdateringen som ble lastet ned til systemet.
3. Flytt installasjonsprogrammet for oppdateringen til mappen C:\Illumina (unntatt fra programvarebegrensingspolicy).
4. Dobbelklikk på installasjonsprogramikonet for å starte grensesnittet.
5. Velg **Remove** (Fjern) for å avinstallere oppdateringen og tilbakestille alle verdier til standardinnstillinger.
6. Velg **Remove** (Fjern) for å bekrefte alternativet for å avinstallere oppdateringen og tilbakestille alle verdier til standardinnstillinger.

 Denne innstillingen vil fjerne systemets beskyttelse og gjøre det sårbart for angrep. Det anbefales på det sterkeste å ta stilling til eventuelle tekniske påvirkninger som fører til at oppdateringen må fjernes, før det tas et valg om å avinstallere.

7. Velg **Finish** (Fullfør) i skjermbildet Installation Completion (Fullfør installasjon).

 | Dersom det kreves verifisering av installasjonsrapport, se [Verifisering på side 5](#).

 | Det anbefales å starte på nytt når installasjonen er fullført.

Verifisering

Hvis det er nødvendig å verifisere installasjonen, vil det ha blitt generert en verifiseringsfil som inneholder dato- og tidsstempel, installert versjon av Local Run Manager og andre viktige verifiseringsverdier. Ta kontakt med techsupport@illumina.com for å få tilgang til denne filen.

Ytterligere anbefalinger for problembegrensning og sikkerhet

Sikker utrulling av RUO-instrumenter og medisinsk Dx-utstyr avhenger av sikkerhetslag. Illumina anbefaler på det sterkeste at instrumenter og enheter kobles til det minste undernett i nettverket eller den minste sikkerhetskonteksten, med pålitelige enheter. Bruk av brannmur og andre nettverkspolycyer for å begrense annen innkommende og utgående tilgang er svært tilrådelig.

Vi anbefaler også:

- Aktiver Transport Layer Security (TLS) (transportlagssikkerhet) for å sørge for at all kommunikasjon utenfor instrumentet er kryptert.
 - Se Local Run Manager Software Guide (programvareveiledningen for Local Run Manager) for informasjon om hvordan du aktiverer Transport Layer Security (TLS) (transportlagssikkerhet).

Andre alternativer

Hvis det av en eller annen grunn ikke er et alternativ å installere oppdateringen, vil følgende manuelle problembegrensningsmetoder redusere risikoen:

- Deaktiver ekstern tilgang til Local Run Manager ved å legge til regler i Windows-brannmuren for å blokkere innkommende tilkoblinger via port 80 og 443.

MSI-installasjonsprogrammet blokkerer automatisk innkommende tilkoblinger i nettserverkonfigurasjonen for Local Run Manager. En manuell problembegrensningsmetode som oppnår samme resultat, er å implementere en konfigurasjon i Windows-brannmuren for å blokkere innkommende tilkoblinger til HTTP (TCP:80) og HTTPS (TLS, TCP:443).

Når dette er implementert, vil Local Run Manager kun være tilgjengelig på datamaskinen der den er installert. Den vil ikke lenger være tilgjengelig fra andre datamaskiner som er tilkoblet samme nettverk.

i | Dersom brukerens arbeidsflyt omfatter å koble seg til Local Run Manager eksternt, vil dette ikke lenger fungere.

- Minimer antallet andre nettverksenheter.

Dersom nettverket konfigureres til å minimere antallet andre nettverksenheter som kan kommunisere med det berørte instrumentet, vil det redusere muligheten for misbruk. Jo færre tilkoblinger som er tilgjengelige for systemet, desto færre muligheter vil være tilgjengelige for tilgang.

Det kan kreve at du konsulterer lokale sikkerhets- eller IT-ressurser.

- Fjern instrumentet fra nettverket.

Hvis ingen andre alternativer er gjennomførbare, er den endelige problembegrensningsmetoden å fjerne instrumentet helt fra nettverket. Dette vil deaktivere tilgangen til Illumina Cloud/SaaS-tjenester som Proactive og BaseSpace® Sequence Hub og vanlige arbeidsflyter for innlasting av genomdata.

Det kan kreve at du konsulterer lokale sikkerhets- eller IT-ressurser.

Undersøkelse av potensiell uautorisert tilgang

Følgende trinn kan hjelpe instrumentoperatøren med å avgjøre om en uautorisert bruker har fått tilgang til systemet:

1. Undersøk IIS-logger som er lagret på `C:\inetpub\logs\LogFiles\W3SVC1` for avvikende betegnelser.
 - Normale betegnelser på Local Run Manager-nettserveren vises slik:

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

- Avvikende betegnelser på Local Run Manager-nettserveren kan vises, for eksempel slik:

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

2. Undersøk IIS-logger for tegn til POST-opplastinger av annet innhold enn manifestfiler. Følgende betegnelser vil for eksempel indikere mistenkelig aktivitet:

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

3. Hvis et antivirusprogram / beskyttelse mot skadelig programvare er installert, bør programvareloggene sjekkes for tegn på avvikende atferd.
4. Undersøk Windows-loggene for tegn på avvikende feilmeldinger.
Hvis en trusselaktør fikk tilgang med administratorrettigheter, vil det være mulig å endre eller slette alle lokale instrumentlogger og -hendelser.

Se etter eventuelle endepunkter systemet kan ha forsøkt å få tilgang til. Se [Control Computer Firewall](#) for en liste over forventede utgående forbindelser.

Kontakt Illuminas tekniske støtte for hjelp hvis nødvendig.

Revisjonshistorikk

| Dokument | Dato | Beskrivelse av endring |
|------------------------------|---------------|--|
| Dokumentnr. 200017330 v02 | April 2022 | La til anbefaling om å utføre oppdateringen når instrumentet ikke kjører. La til instruksjon om at en omstart av instrumentet er nødvendig etter installering av oppdatering. Korrigerende revisjonshistorikkbeskrivelsen for v01. |
| Dokumentnr. 200017330 v01 | April 2022 | Endret dokumentnavn på veiledning for LRM-programvareoppdatering 1.0. Fjernet referanser til v1.0.1. La til avsnitt for å dekke undersøkelsen av potensiell uautorisert tilgang. |
| Dokumentnr. 200017330 v00 | Mars 2022 | Første versjon. |

Dette dokumentet og dets innhold er opphavsrettslig beskyttet for Illumina, Inc. og tilknyttede selskaper («Illumina»), og er ment utelukkende for kontraktbruk av kunden i forbindelse med bruk av produktet (produktene) beskrevet her, og for intet annet formål. Dette dokumentet og dets innhold skal ikke brukes eller distribueres til andre formål og/eller på annen måte kommuniseres, fremlegges eller reproduseres på noen måte uten forutgående, skriftlig samtykke fra Illumina. Illumina overfører ikke noen lisens under sitt patent, varemerke, opphavsrett eller sedvanerett eller lignende rettigheter til tredjeparter gjennom dette dokumentet.

Instruksjonene i dette dokumentet skal følges strengt og tydelig av kvalifisert og tilfredsstillende utdannet personell for å sikre riktig og sikker bruk av produktet (produktene) som er beskrevet i dette dokumentet. Alt innhold i dette dokumentet skal leses fullt ut og være forstått før produktet (produktene) brukes.

HVIS DET UNNLATES Å LESE FULLSTENDIG OG UTTRYKKELEG FØLGE ALLE INSTRUKSJONENE I DETTE DOKUMENTET, KAN DET FØRE TIL SKADE PÅ PRODUKTET (PRODUKTENE), SKADE PÅ PERSONER, INKLUDERT BRUKERE ELLER ANDRE, OG SKADE PÅ ANNEN EIENDOM, OG DETTE VIL UGYLDIGGJØRE EVENTUELL GARANTI SOM GJELDER FOR PRODUKTET (PRODUKTENE).

ILLUMINA PÅTAR SEG IKKE ANSVAR SOM FØLGE AV FEIL BRUK AV PRODUKTET (PRODUKTENE) SOM ER BESKREVET I DETTE DOKUMENTET (INKLUDERT DELER AV DETTE ELLER PROGRAMVARE).

© 2022 Illumina, Inc. Med enerett.

Alle varemerker tilhører Illumina, Inc. eller deres respektive eiere. Ytterligere informasjon om varemerker finner du på www.illumina.com/company/legal.html.