LRM-softwarepatch 1.0

illumina®

Instructiehandleiding

Inleiding

Illumina® heeft kennis genomen van een kwetsbaarheid in de beveiliging van de Local Run Manager-software en heeft een softwarepatch geleverd om te beschermen tegen extern misbruik van deze kwetsbaarheid.

Local Run Manager is een autonome software-applicatie en maakt deel uit van de standaardconfiguratie van de volgende systemen:

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

*Bestemd voor in-vitrodiagnostiek.

Deze handleiding is van toepassing op de hierboven genoemde Illumina-instrumenten en ook op de computers buiten de instrumenten waarop de autonome versie van Local Run Manager is geïnstalleerd.

De kwetsbaarheid is een 'Unauthenticated Remote Command Execution' (RCE, een niet-geverifieerde uitvoering van een externe opdracht) met een onbeperkte CVSS-score van 10.0 Critical, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

De volgende beperkende maatregelen zijn nodig bij de bovengenoemde instrumenten om ze te beveiligen tegen de mogelijkheid dat een niet-geautoriseerd persoon toegang krijgt tot een of meer instrumenten en deze op afstand aanvalt.

Als het installatieprogramma om wat voor reden dan ook niet kan worden uitgevoerd, raadpleeg dan de paragraaf over aanvullende beperkingen aan het einde van dit document of neem contact op met techsupport@illumina.com voor verdere hulp.

Zie De Local Run Manager-update verkrijgen voor opties voor het downloaden of aanvragen van een kopie van de patch.

- **v1.0.0 patch** – hiermee wordt de Local Run Manager-webconfiguratie geüpdatet en toegang tot externe Internet Information Services (IIS) uitgeschakeld.

De Local Run Manager-beveiligingspatch bemachtigen

Er zijn vier (4) opties voor het bemachtigen van de Local Run Manager-beveiligingspatch.

Optie 1—Rechtstreeks naar uw instrument downloaden

De snelste manier om de Local Run Manager-beveiligingsupdate te verkrijgen is door deze rechtstreeks vanaf de hostwebsite te downloaden naar het instrument.

1. Download het installatieprogramma voor de patch via de link die via een beveiligde e-mail naar uw instrument is gestuurd.
2. Draag het bestand over naar de map `C:\Illumina` op het instrument.
3. Volg de instructies in *De Local Run Manager-beveiligingspatch toepassen* op pagina 4.

Optie 2—Het installatieprogramma voor de patch downloaden naar de computer en overdragen naar het instrument via een USB-stick/gedeelde map

Als u de beveiligingspatch niet kunt downloaden naar het instrument, raden we u aan het naar een afzonderlijke computer te downloaden en vervolgens over te dragen naar het instrument.

Controleer met uw beveiligingsmedewerkers voor gebruik de integriteit van de USB-stick. (Aanbevolen)

1. Download het installatieprogramma voor de patch via de link die via een beveiligde e-mail naar uw computer of laptop is gestuurd.
2. Kopieer het gedownloade installatieprogramma voor de patch vanaf de computer naar een USB-stick of gedeelde map.
3. Bij een USB-stick: plaats de stick in het instrument.
4. Kopieer het installatieprogramma voor de patch van de USB-stick of de gedeelde map naar de map `C:\Illumina` op het instrument.
5. Volg de instructies in *De Local Run Manager-beveiligingspatch toepassen* op pagina 4.

Optie 3—Technische hulp vragen

Een medewerker van de technische dienst van Illumina zal u door het patchproces leiden aan de hand van een van de volgende methoden:

- Inloggen op afstand door de technische medewerker

  Een medewerker van de technische dienst kan op afstand inloggen bij de analyzer en de patch voor de klant installeren.

  Het systeem moet dan wel toegankelijk zijn van buitenaf. Mocht u vragen hebben, vraag dan uw lokale IT-medewerker om hulp.

- Begeleide instructies
  Een medewerker van de technische dienst biedt begeleide instructies via de telefoon. Neem contact op met uw lokale medewerker van de technische dienst voor hulp.

Optie 4—Een vooraf geconfigureerde USB-stick bestellen bij Illumina

Klanten kunnen gratis een tegen overschrijven beveiligde USB-stick bestellen. Neem contact op met techsupport@illumina.com om de stick met de patch te bestellen.

Er kan sprake zijn van vertragingen bij verzending of in de voorraad die invloed hebben op de tijdigheid van de levering. Om systemen sneller te beschermen wordt sterk aanbevolen de systemen te beschermen via de methode die de meest efficiënte weg naar een oplossing biedt.

Het installatieprogramma voor de Local Run Manager-beveiligingspatch v.1.0 toepassen

De MSI (Microsoft Installer) van Illumina zal als het wordt uitgevoerd, de Local Run Manager-webserverconfiguratie bijwerken om uitvoering van door een gebruiker geüploade content te voorkomen en de externe toegang tot de Local Run Manager-webinterface vanaf LAN-netwerkverbindingen volledig te blokkeren.

Voor gebruikers die werken met de Local Run Manager-webinterface voor externe toegang tot instrumenten, werkt deze workflow niet meer na installatie van deze patch. Illumina is van plan deze functie later te herstellen bij de permanente softwarefix voor dit probleem. Als dit zorgt voor een onderbreking van bestaande workflows, neem dan contact op met techsupport@illumina.com voor verdere hulp.

De MSI Installer is van toepassing op alle versies van Local Run Manager en bepaalt automatisch de juiste fix op basis van de Local Run Manager-versie die is geïnstalleerd op het instrument/de computer.

Deze MSI Installer maakt ook een auditbestand waarin staat dat deze beperking is toegepast, met een tijdstempel die de correcte installatie aangeeft.

De MSI Installer uitvoeren – de eerste keer dat de MSI Installer wordt uitgevoerd, zal het installatieprogramma het systeem herstellen en een auditbestand maken met de voltooiingstijd.

Als de MSI Installer nogmaals wordt uitgevoerd, wordt een **Herstel**-optie gepresenteerd. De gebruiker heeft dan de mogelijkheid om de patch opnieuw toe te passen of terug te draaien. Opmerking: De patch terugdraaien resulteert in een onveilige instrumentconfiguratie.

De Local Run Manager-beveiligingspatch toepassen

De patch installeren:

1. Log in bij het systeem via een beheerdersaccount (bijv. sbsadmin).

   Illumina raadt aan de patch toe te passen als het instrument niet in gebruik is. Als het instrument een run uitvoert, moet de patch onmiddellijk na afloop van de run worden toegepast.

2. Vind de patch die naar het systeem is gedownload.
3. Verplaats het installatieprogramma voor de patch naar de map `C:\Illumina` (vrijgesteld van het softwarebeperkingsbeleid).
4. Dubbelklik op het installatiepictogram om de interface te starten.
5. Selecteer als de applicatie wordt geladen '**Next**' (Volgende) om te beginnen met de installatie van de patch.
6. Selecteer **Finish** (Voltooien) op het scherm 'Installation Completion' (Installatie afronden).

Zie *Verificatie* op pagina 5 als een rapport voor verificatie van de installatie nodig is.

Aan het einde van de installatie is een reboot nodig.

Herstellen

In het geval van een fout kan de klant een herstel van de installatie uitvoeren door de onderstaande instructies te volgen:

1. Log in bij het systeem via een beheerdersaccount (bijv. sbsadmin).
2. Vind de patch die naar het systeem is gedownload.
3. Verplaats het installatieprogramma voor de patch naar de map `C:\Illumina` (vrijgesteld van het softwarebeperkingsbeleid).
4. Dubbelklik op het installatiepictogram om de interface te starten.
5. Het installatieprogramma detecteert automatisch of de configuratietool eerder is uitgevoerd en geeft nieuwe opties weer:
   a. 'Change' (Wijzigen): Grijs en niet beschikbaar
   b. 'Repair' (Herstellen): Herstelt fouten en biedt opties voor een nieuwe configuratie.
   c. 'Remove' (Verwijderen): De-installeert de patch en herstelt de standaardconfiguratie (zie *De-installeren* op pagina 5)
6. Selecteer **Finish** (Voltooien) op het scherm 'Installation Completion' (Installatie afronden).

Zie *Verificatie* op pagina 5 als een rapport voor verificatie van de installatie nodig is.

Aan het einde van de installatie is een reboot nodig.

De-installeren

Het de-installeren van de patch draait de aanpassingen die aan het host-configuratiebestand van de applicatie zijn aangebracht.

1. Log in bij het systeem via een beheerdersaccount (bijv. sbsadmin).
2. Vind de patch die naar het systeem is gedownload.
3. Verplaats het installatieprogramma voor de patch naar de map `C:\Illumina` (vrijgesteld van het softwarebeperkingsbeleid).
4. Dubbelklik op het installatiepictogram om de interface te starten.
5. Selecteer **Remove** (Verwijderen) om de patch te de-installeren en alle waarden terug te zetten naar de standaardinstellingen.
6. Selecteer **Remove** (Verwijderen) om de optie voor het de-installeren van de patch te bevestigen en alle waarden terug te zetten naar de standaardinstellingen.

Door deze instelling wordt het systeem onveilig: het loopt meer risico om te worden aangevallen. Het wordt sterk aanbevolen om de technische gevolgen van uw keuze om de patch te verwijderen op te lossen voordat u kiest voor de-installatie.

7. Selecteer **Finish** (Voltooien) op het scherm 'Installation Completion' (Installatie afronden).

Zie *Verificatie* op pagina 5 als een rapport voor verificatie van de installatie nodig is.

Een reboot aan het einde van de installatie wordt aanbevolen.

Verificatie

Als het nodig is de installatie te verifiëren, dan is er een verificatiebestand gegenereerd met een datum en tijdstempel, de versie van de geïnstalleerde Local Run Manager en andere belangrijke verificatiewaarden. Neem contact op met techsupport@illumina.com om dit bestand aan te vragen.

Aanvullende aanbevelingen voor risicobeperking en beveiliging

Veilig gebruik van RUO-instrumenten en diagnostische (Dx) medische hulpmiddelen is afhankelijk van de lagen van beveiliging. Illumina beveelt sterk aan instrumenten en apparaten in het kleinste subnet van een netwerk of de kleinste veiligheidscontext te gebruiken, samen met vertrouwde apparaten. Het gebruik van firewalls en andere maatregelen om het overige inkomende/uitgaande netwerkverkeer te beperken wordt zeer aangeraden.

Wij raden ook het volgende aan:

- Schakel Transport Layer Security (TLS) in om er zeker van te zijn dat alle communicatie buiten het instrument versleuteld is.
  - Raadpleeg de softwarehandleiding van Local Run Manager voor informatie over het inschakelen van Transport Layer Security (TLS).

Alternatieve opties

Als uitvoering van de patch om wat voor reden dan ook niet mogelijk is, verkleinen de volgende handmatige beperkingsmethoden het risico:

- Schakel toegang op afstand tot Local Run Manager uit door Windows-firewallregels voor het blokkeren van inkomende verbindingen met poort 80 en 443 toe te voegen.
  De MSI Installer blokkeert automatisch externe inkomende verbindingen in de webserverconfiguratie van Local Run Manager. Een handmatige beperking die hetzelfde resultaat bereikt, is het toepassen van een Windows-firewallconfiguratie voor het blokkeren van inkomende verbindingen met `HTTP-verbindingen (TCP:80)` en `HTTPS-verbindingen (TLS, TCP:443)`.
  Als deze beperking wordt toegepast, is Local Run Manager alleen toegankelijk op de computer waarop het is geïnstalleerd. Het is dan niet meer toegankelijk via andere computers die op hetzelfde netwerk zijn aangesloten.

> Als de gebruikersworkflow externe toegang tot Local Run Manager omvat, zal deze functionaliteit niet meer werken.

- Beperk het aantal andere netwerkapparaten tot een minimum.
  Met een netwerkconfiguratie waardoor het aantal andere apparaten dat met het betreffende instrument kan communiceren tot een minimum wordt beperkt, verkleint u de mogelijkheden tot misbruik. Hoe minder verbindingen er beschikbaar zijn voor het systeem, hoe minder toegangsmogelijkheden er zijn.
  Het kan nodig zijn om voor uitvoering hiervan te overleggen met uw locale informatiebeveiligings- of IT-medewerkers.
- Verwijder het instrument uit het netwerk.
  Als er geen andere optie mogelijk is, is de laatste beperking het volledig verwijderen van het instrument uit het netwerk. Hiermee wordt de toegang tot Illumina Cloud/SaaS-diensten zoals Proactive en de BaseSpace® Sequence Hub en tot typische workflows voor het verladen van genomische gegevens uitgeschakeld.
  Het kan nodig zijn om voor uitvoering hiervan te overleggen met uw locale informatiebeveiligings- of IT-medewerkers.

Onderzoek naar mogelijk ongeoorloofde toegang

De volgende stappen zijn de operator van het instrument mogelijk van dienst bij het bepalen of een ongeoorloofde gebruiker toegang heeft gehad tot het systeem:

1. Onderzoek de IIS-logboeken die zijn opgeslagen in `C:\inetpub\logs\LogFiles\W3SVC1` op afwijkende bepalingen.
   - Normale bepalingen naar de Local Run Manager-webserver zien er als volgt uit:

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

   - Afwijkende bepalingen naar de Local Run Manager-webserver kunnen er bijvoorbeeld als volgt uitzien:

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

2. Onderzoek het IIS-logbestand op tekenen van POST-uploads met andere content dan manifestbestanden. Bijvoorbeeld, de volgende bepalingen wijzen op verdachte activiteiten:

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

3. Als een antivirus-/anti-malwaretoepassing is geïnstalleerd, moet u de softwarelogboeken controleren op tekenen van afwijkend gedrag.
4. Onderzoek de vensterlogboeken op tekenen van afwijkende foutberichten.
   Als een bedreigende partij toegang heeft gekregen met beheerdersrechten, dan heeft deze partij de mogelijkheid alle lokale instrumentlogboeken en -gebeurtenissen te wijzigen of te verwijderen.

Controleer op eindpunten die het systeem heeft geprobeerd te bereiken. Raadpleeg Firewall besturingscomputer voor een lijst met verwachte uitgaande verbindingen.

Neem indien nodig contact op met de technische ondersteuning van Illumina voor hulp.

Revisiegeschiedenis

Document	Datum	Omschrijving van wijziging
Documentnr. 200017330 v02	April 2022	Aanbeveling toegevoegd de patch toe te passen als het instrument niet wordt gebruikt. Instructie toegevoegd dat een reboot van het instrument nodig is na installatie van de patch. De omschrijving van de revisiegeschiedenis voor v01 gecorrigeerd.
Documentnr. 200017330 v01	April 2022	Titel document veranderd naar LRM-softwarepatch 1.0 Instructiehandleiding Alle verwijzingen naar v1.0.1 verwijderd. Sectie toegevoegd dat het onderzoek naar mogelijk ongeoorloofde toegang omvat.
Documentnr. 200017330 v00	Maart 2022	Eerste uitgave.