LRM Software Patch 1.0

illumina®

Användarhandbok

Inledning

Illumina® har blivit medveten om en säkerhetsrisk i Local Run Manager-programvaran och har utvecklat en programfix för att skydda mot fjärrutnyttjanden av den här sårbarheten.

Local Run Manager är ett fristående program och en del av standardkonfigurationen av följande system:

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

*För in vitro-diagnostiskt bruk.

Den här handboken gäller Illumina-instumenten som listas ovan och datorer utanför instrumentet som har den fristående versionen av Local Run Manager installerad.

Säkerhetsrisken är en oautentiserad Remote Command Execution (RCE) med ett totalt CVSS-resultat på 10,0 Critical, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Följande åtgärdssteg måste användas på alla instrument som listas ovan för att skydda mot risken att en obehörig användare får tillgång till ett eller flera instrument och utför en fjärråtkomstattack.

Om installationsprogrammet av någon anledning inte kan köras hittar du mer information i avsnittet om ytterligare åtgärder i slutet av det här dokumentet. Du kan även kontakta techsupport@illumina.com för ytterligare hjälp.

Alternativ för hur du kan ladda ner eller begära en kopia av programfixen finns i avsnittet Ladda ner Local Run Manager-uppdateringen.

- **v1.0.0 patch** (Uppdatering v1.0.0) – Det här alternativet kommer att uppdatera Local Run Manager-webbkonfigurationen och inaktivera fjärråtkomst till Internet Information Services (IIS).

Erhålla Local Run Manager Security Patch

Det finns fyra (4) alternativ för att erhålla Local Run Manager Security Patch.

Alternativ 1 – Ladda ner direkt till instrumentet

Det snabbaste sättet att erhålla Local Run Manager Security Update på är att ladda ner den direkt från värdwebbplatsen till instrumentet.

1. Ladda ner programfixens installationsprogram med länken som tillhandahålls via säker e-post till ditt instrument.
2. Överför filen till mappen `C:\Illumina` på instrumentet.
3. Följ anvisningarna i avsnittet *Installera Local Run Manager Security Patch* på sidan 4.

Alternativ 2 – Ladda ner programfixens installationsprogram till datorn och överföra det till instrumentet via en USB-enhet/delad mapp

Om du inte kan ladda ner säkerhetsuppdateringen till instrumentet rekommenderar vi att du laddar ner den till en separat dator och sedan överför den till instrumentet.

Verifiera att det är säkert att använda USB-enheten med de säkerhetsansvariga innan du använder den (rekommenderas).

1. Ladda ner programfixens installationsprogram med länken som tillhandahålls via säker e-post till din dator eller bärbara dator.
2. Kopiera programfixens nedladdade installationsprogram till USB-enheten eller den delade mappen från datorn.
3. Om du använder en USB-enhet ska du ansluta enheten till instrumentet.
4. Kopiera programfixens installationsprogram från USB-enheten eller den delade mappen till mappen `C:\Illumina` på instrumentet.
5. Följ anvisningarna i avsnittet *Installera Local Run Manager Security Patch* på sidan 4.

Alternativ 3 – Begär teknisk support

Illuminas tekniska support guidar dig genom uppdateringsprocessen med en av följande metoder:

- Fjärrinloggning för teknisk support
  Den tekniska supporten kan då fjärransluta till analysatorn och installera programfixen åt kunden.

  Det måste vara möjligt att få åtkomst till systemet från fjärrdatorer. Kontakta din lokala IT-representant om du har frågor.

- Guidade anvisningar
  Den tekniska supporten ger guidade anvisningar över telefon. Kontakta din lokala tekniska support om du har frågor.

Alternativ 4 – Beställ en förkonfigurerad enhet från Illumina

Kunden kan beställa en skrivskyddad USB-enhet utan kostnad. Kontakta techsupport@illumina.com om du vill beställa en USB-enhet med programfixen.

Leveranstiden kan påverkas av försenade leveranser och lagerstatus. För att systemen ska få ett mer omedelbart skydd rekommenderar vi starkt att de skyddas med den metod som går snabbast att tillämpa.

Använda installationsprogrammet föt Local Run Manager Security Patch v.1.0

Illuminas MSI (Microsoft Installer) kommer, när det körs, att uppdatera konfigurationen av Local Run Manager-webbservern för att förhindra att innehåll som laddats upp av användare körs och blockera all fjärråtkomst till Local Run Manager-webbgränssnittet från LAN-nätverksanslutningar.

För de användare som använder Local Run Manager-webbgränssnittet för att få fjärråtkomst till instrument kommer arbetsflödet inte länge att fungera när den här programfixen har installerats. Illumina avser att återställa den här funktionen med en permanent programfixen för problemet vid ett senare tillfälle. Om det här orsakar ett avbrott i etablerade arbetsflöden ska du kontakta techsupport@illumina.com för ytterligare hjälp.

MSI Installer kan användas med alla versioner av Local Run Manager och kommer automatiskt att fastställa rätt åtgärd baserat på den Local Run Manager-version som är installerad på instrumentet/datorn.

MSI Installer kommer även att skapa en granskningsfil som visar att åtgärden har implementerats och en tidsstämpel för att det ska vara möjligt att verifiera att installationen utfördes korrekt.

Köra MSI Installer – Första gången MSI Installer körs kommer installationsprogrammet att uppdatera systemet och skapa en granskningsfil med slutförandetiden.

Om MSI Installer körs igen kommer alternativet **Repair** (Reparera) att visas. Användaren kan då välja att köra installationsprogrammet igen eller återställa uppdateringen. Obs! Om programfixen återställs kommer inte instrumentkonfigurationen att vara säker.

Installera Local Run Manager Security Patch

Så här installerar du programfixen:

1. Logga in på systemet via ett administratörskonto (t.ex. sbsadmin).

   Illumina rekommenderar att programfixen installeras när instrumentet inte används. Om instrumentet utför en körning bör programfixen installeras omedelbart efter att körningen har slutförts.

2. Hitta programfixen som laddades ner till systemet.
3. Flytta programfixens installationsprogram till mappen `C:\Illumina` (undantagen från principen som begränsar programvaran).
4. Dubbelklicka på installationsikonen för att starta gränssnittet.
5. Välj **Next** (Nästa) när programmet har startats för att påbörja installationen av programfixen.
6. Välj **Finish** (Slutför) på skärmen Installation Completion (Slutför installation).

Om installationsrapporten behöver verifieras hittar du mer information i avsnittet *Verifiering* på sidan 5 (Verifiering).

Instrumentet måste startas om efter installationen.

Reparera

Om det uppstår ett fel kan kunden reparera installationen genom att följa anvisningarna nedan:

1. Logga in på systemet via ett administratörskonto (t.ex. sbsadmin).
2. Hitta programfixen som laddades ner till systemet.
3. Flytta programfixens installationsprogram till mappen `C:\Illumina` (undantagen från principen som begränsar programvaran).
4. Dubbelklicka på installationsikonen för att starta gränssnittet.
5. Installationsprogrammet kommer automatiskt att upptäcka om konfigurationsverktyget har körts tidigare och ge dig nya alternativ:
   a. Change (Ändra): Gråtonat och inte tillgängligt.
   b. Repair (Reparera): Reparerar fel och ger alternativ för omkonfigurering.
   c. Remove (Ta bort): Avinstallerar programfixen och återställer systemet till standardkonfigurationen (mer information finns i avsnittet *Avinstallation* på sidan 5).
6. Välj **Finish** (Slutför) på skärmen Installation Completion (Slutför installation).

Om installationsrapporten behöver verifieras hittar du mer information i avsnittet *Verifiering* på sidan 5 (Verifiering).

Instrumentet måste startas om efter installationen.

Avinstallation

Om programfixen avinstalleras kommer de ändringar som gjorts i programvärdens konfigurationsfil att återställas.

1. Logga in på systemet via administratörskontot (t.ex. sbsadmin).
2. Hitta programfixen som laddades ner till systemet.
3. Flytta programfixens installationsprogram till mappen `C:\Illumina` (undantagen från principen som begränsar programvaran).
4. Dubbelklicka på installationsikonen för att starta gränssnittet.
5. Välj **Remove** (Ta bort) för att avinstallera programfixen och återställa alla värden till standardinställningarna.
6. Välj **Remove** (Ta bort) för att bekräfta ditt val att avinstallera programfixen och återställa alla värden till standardinställningarna.

Den här inställningen kommer att göra systemet osäkert och öka risken för attacker. Vi rekommenderar starkt att alla tekniska konsekvenser som leder till att programfixen avinstalleras åtgärdas innan du väljer att avinstallera programfixen.

7. Välj **Finish** (Slutför) på skärmen Installation Completion (Slutför installation).

Om installationsrapporten behöver verifieras hittar du mer information i avsnittet *Verifiering* på sidan 5 (Verifiering).

Vi rekommenderar att du startar om instrumentet efter installationen.

Verifiering

Om installationen behöver verifieras finns det en verifieringsfil som inkluderar en datum- och tidsstämpel, installerad version av Local Run Manager och andra viktiga verifieringsvärden. Kontakta techsupport@illumina.com om du vill få filen.

Ytterligare åtgärds- och säkerhetsrekommendationer

Säker användning av RUO-instrument och medicinska Dx-enheter är beroende av flera lager av säkerhet. Illumina rekommenderar starkt att instrument och enheter används i den minsta nätverksundergruppen eller säkerhetskontexten, med betrodda enheter. Vi rekommenderar starkt att brandväggar och andra nätverkspolicyer används för att begränsa att annan inkommande och utgående trafik får åtkomst till instrumenten eller enheterna.

Vi rekommenderar även följande:

- Aktivera Transport Layer Security (TLS) för att säkerställa att all kommunikation utanför instrumentet är krypterad.
  - Information om hur du aktiverar Transport Layer Security (TLS) finns i Local Run Manager Software Guide (Programhandbok för Local Run Manager).

Andra alternativ

Om det av någon anledning inte är ett alternativ att installera programfixen kommer följande manuella åtgärdsmetoder att minska risken:

- Inaktivera fjärråtkomst till Local Run Manager genom att lägga till Windows-brandväggsregler för att blockera inkommande anslutningar via port 80 och 443.
  MSI Installer kommer automatiskt att blockera inkommande fjärranslutningar i Local Run Manager-webbserverkonfigurationen. En manuell åtgärd som får samma resultat är att implementera en Windows-brandväggskonfiguration för att blockera inkommande anslutningar till `HTTP- (TCP:80)` och `HTTPS-anslutningar (TLS, TCP:443)`.
  När den har implementerats kan Local Run Manager endast användas på den dator som Local Run Manager är installerat på – det kommer inte längre att vara tillgängligt från andra datorer som är anslutna till samma nätverk.

> Om användarens arbetsflöde involverar fjärråtkomst till Local Run Manager kommer den här funktionen inte längre att fungera.

- Minimera antalet andra nätverksenheter.
  Att konfigurera nätverket för att minimera antalet andra nätverksenheter som kan kommunicera med det berörda instrumentet kommer att minska risken för att nätverket utnyttjas. Ju färre anslutningar som är tillgängliga för systemet, desto färre åtkomstmöjligheter finns det.
  Du kan behöva kontakta dina lokala informationssäkerhets- eller IT-resurser för att utföra den här åtgärden.
- Ta bort instrumentet från nätverket.
  Den sista åtgärden är att ta bort instrumentet från nätverket. Det inaktiverar åtkomst till Illumina Cloud-/SaaS-tjänster som Proactive och BaseSpace® Sequence Hub, samt typiska arbetsflöden för genomisk dataavlastning.
  Du kan behöva kontakta dina lokala informationssäkerhets- eller IT-resurser för att utföra den här åtgärden.

Utredning av potentiell obehörig åtkomst

Följande steg kan hjälpa instrumentets användare att avgöra om en obehörig användare har fått åtkomst till systemet:

1. Kontrollera IIS-loggarna som är lagrade i `C:\inetpub\logs\LogFiles\W3SVC1` för avvikande anrop.
   - Vanliga anrop till Local Run Manager-webbservern ser ut så här:

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

   - Avvikande anrop till Local Run Manager-webbservern kan visas. Tiil exempel:

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

2. Kontrollera IIS-loggen för tecken på POST-uppladdningar som inte är manifestfiler. Anropen nedan är exempelvis tecken på misstänkt aktivitet:

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

3. Om ett antivirusprogram eller program mot skadlig kod har installerats ska programvaruloggarna kontrolleras för att se om det finns tecken på avvikande händelser.
4. Kontrollera Windows-loggarna för tecken på avvikande felmeddelanden.
   Om fientliga aktörer lyckas få tillgång till de administrativa rättigheterna kan de ändra eller ta bort alla lokala instrumentloggar och händelser.

Kontrollera eventuella slutpunkter som systemet kan ha försökt nå. En lista över förväntade utgående anslutningar finns på Control Computer Firewall.

Kontakta Illuminas tekniska support för hjälp.

Revisionshistorik

Dokument	Datum	Ändringsbeskrivning
Dokumentnr 200017330 v02	April 2022	En rekommendation om att installera programmet när instrumentet inte är igång har lagts till. Anvisningar om att instrumentet måste startas om efter att programfixen har installerats har lagts till. Beskrivningen av versionshistoriken för v01 har rättats.
Dokumentnr 200017330 v01	April 2022	Dokumentnamnet har ändrats till Användarhandbok för LRM Software Patch 1.0. Ingen referens görs till v1.0.1. Ett avsnitt om utredningen av potentiell obehörig åtkomst har lagts till.
Documentnr 200017330 v00	Mars 2022	Första utgåvan.