LRM-Softwarepatch 1.0

illumina®

Instruktiounsguide

Aleedung

Illumina® huet eng Sécherheetsschwaachstell an der "Local Run Manager"-Software entdeckt an e Softwarepatch bereetgestallt, fir géint d'Fernausnotzung vun dëser Schwaachstell ze schützen.

Local Run Manager ass eng eegestänneg Softwareapplikatioun an Deel vun der Standardkonfiguratioun op de follgende Systemer:

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

*Fir In-Vitro-Diagnostik.

Dëst Handbuch gëllt fir déi uewen opgelëscht Illumina-Instrumenter an och fir Computere baussent dem Instrument, op deenen déi eegestänneg Versioun vu Local Run Manager installéiert ass.

Bei der Schwaachstell handelt et sech ëm eng net authentifizéiert Remotebefeelsausféierung (RCE) mat engem direkten CVSS-Score vun 10.0 Kritesch, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Déi follgend Moossnamen zur Risikoverréngerung sinn op den uewen opgelëschten Instrumenter erfuerderlech, fir géint d'Méiglechkeet ze schützen, datt en net autoriséierte Benotzer Zougréff op een oder méi Instrumenter kritt an e Remotezougréffsugréff ausféiert.

Wann den Installatiounsprogramm aus iergendengem Grond net ausgeféiert ka ginn, da liest den Abschnitt "Zousätzlech schuedensbegrenzend Moossnamen" um Enn vun dësem Dokument oder went Iech un techsupport@illumina.com fir weider Ënnerstëtzung ze kréien.

Consultéiert Ofruffe vun der Local-Run-Manager-Aktualiséierung fir Optiounen, wéi eng Kopie vum Patch erofgelueden oder ugefuerdert ka ginn.

- **v1.0.0-Patch** – aktualiséiert d'Local-Run-Manager-Webkonfiguratioun an desaktivéiert de Remotezougréff op Internet Information Services (IIS).

De Local-Run-Manager-Sécherheetspatch ofruffen

Et gi véier (4) Optioune fir de "Local Run Manager"-Patch ofzeruffen.

Optioun 1 – Direkt op Äert Instrument eroflueden

Am séierste kritt Dir d'Local-Run-Manager-Sécherheetsaktualiséierung, wann Dir se direkt vum Hostingsite op d'Instrument erofluet.

1. Luet de Patchinstallatiounsprogramm iwwer de Link, dee per sécherer E-Mail bereetgestallt gëtt, op Äert Instrument erof.
2. Iwwerdrot d'Datei an den Dossier `C:\Illumina` um Instrument.
3. Befollegt d'Instruktiounen ënner *De Local-Run-Manager-Sécherheetspatch uwenden* op Säit 4.

Optioun 2 – Luet de Patchinstallatiounsprogramm op de Computer erof an iwwerdrot en iwwer en USB-Lafwierk oder e gedeelten Dossier op d'Instrument.

Wann Dir de Sécherheetspatch net op d'Instrument erofluede kënnt, empfiele mir, en op en separate Computer erofzelueden an dann op d'Instrument ze iwwerdroen.

Iwwerpréift d'Integritéit vum USB-Lafwierk virun der Verwendung mat Ärem Sécherheetsbeoptraagten. (Empfuel)

1. Luet de Patchinstallatiounsprogramm iwwer de Link, dee per sécherer E-Mail bereetgestallt gëtt, op Äre Computer oder Laptop erof.
2. Kopéiert den erofgeluedene Patchinstallatiounsprogramm vum Computer op d'USB-Lafwierk oder de gedeelten Dossier.
3. Schléisst d'Lafwierk fir en USB-Lafwierk un d'Instrument un.
4. Kopéiert de Patchinstallatiounsprogramm vum USB-Lafwierk oder dem gedeelten Dossier an den Dossier `C:\Illumina` um Instrument.
5. Befollegt d'Instruktiounen ënner *De Local-Run-Manager-Sécherheetspatch uwenden* op Säit 4.

Optioun 3 – Technesch Ënnerstëtzung ufroen

E Mataarbechter vun der technescher Ënnerstëtzung vun Illumina féiert lech duerch de Patchprozess mat Hëllef vun enger vun de follgende Methoden:

- Fernzougréff duerch den Tech Support

  E Mataarbechter vum techneschen Support gräift aus der Distanz op den Analyzer zou an installéiert de Patch am Numm vum Client.

  De System muss extern zougänglech sinn. Wann Dir Froen hutt, da went lech un Ären IT-Mataarbechter um Site.

- Geféiert Instruktiounen
  E Mataarbechter vum Tech Support gëtt lech Instruktiounen iwwer den Telefon. Kontaktéiert wgl. Äre lokale Mataarbechter vum Tech Support fir Ënnerstëtzung.

Optioun 4 – E virkonfiguréiert Lafwierk bei Illumina bestellen

E schreifgeschützt USB-Lafwierk ka gratis vum Client bestallt ginn. Fir d'Lafwierk mam installéierte Patch ze bestellen, went lech wgl. un techsupport@illumina.com.

Et kann zu Verzögerunge bei Liwwerungen oder Bestänn kommen, déi sech op d'Aktualitéit vun der Liwwerung auswierke kënnen. Fir Systemer direkt ze schützen, gëtt dréngend empfuel, Systemer mat där Method ze schützen, déi den effizientste Léisungswee bitt.

Installéiert den Installatiounsprogramm fir de Local-Run-Manager-Sécherheetspatch v.1.0.

Den Illumina-MSI (Microsoft-Installatiounsprogramm) aktualiséiert bei der Ausféierung d'Konfiguratioun vum Local-Run-Manager-Webserver, fir d'Ausféierung vu vum Benotzer eropgelueden Inhalter ze verhënneren an de Remotezougréff op de Local-Run-Manager-Webinterface iwwer LAN-Netzwierkverbindungen ze blockéieren.

Fir Benotzer, déi de Local-Run-Manager-Interface fir de Fernzougréff op Apparater verwenden, funktionéiert dësen Aarbechtsoflaf no der Installatioun vun dësem Patch net méi. Illumina huet vir, dës Funktionalitéit mat der permanenter Softwarefeelerbehiewung fir dëse Problem spéider nees hirzestellen. Wann dat zu enger Ënnerbriechung vun existenten Aarbechtsofleef féiert, da went lech wgl. un techsupport@illumina.com, fir weider Ënnerstëtzung ze kréien.

Den MSI-Installatiounsprogramm gëllt fir all Versioune vu Local Run Manager an ermëttelt automatesch déi richteg Feelerbehiewung baséierend op der um Apparat/Computer installéierter Local-Run-Manager-Versioun.

Den MSI-Installatiounsprogramm erstellt och eng Iwwerwaachungsdatei, déi weist, datt dës Risikoverréngerung implementéiert gouf, zesumme mat engem Zäitstempel, deen déi uerdnungsgeméiss Installatioun uweist.

Ausféiere vum MSI-Installatiounsprogramm – bei der éischter Ausféierung vum MSI-Installatiounsprogramm erstellt den Installatiounsprogramm e Patch fir de System an eng Iwwerwaachungsdatei mat der Ofschlosszäit.

Wann Dir den MSI-Installatiounsprogramm erneit ausféiert, gëtt eng **Reparaturoptioun** ugewisen. De Benotzer huet d'Méiglechkeet, de Patch erneit unzewenden oder zeréckzesetzen. Hiweis: E Rollback vum Patch féiert zu enger onsécherer Instrumentkonfiguratioun.

De Local-Run-Manager-Sécherheetspatch uwenden

Fir de Patch ze installéieren:

1. Mellt lech iwwer en Administrateurskont (z. B. sbsadmin) um System un.

   Illumina empfielt, de Patch unzewenden, wann d'Instrument net a Betrib ass. Wann d'Instrument en Duerchlaf ausféiert, sollt de Patch direkt nom Ofschloss vum Duerchlaf ugewant ginn.

2. Sicht de Patch, deen op de System erofgeluede gouf.
3. Réckelt de Patchinstallatiounsprogramm an den Dossier `C:\Illumina` (ass vun der Softwareaschränkungsrichtlinn ausgeholl).
4. Duebelklickt op d'Installatiounsprogrammsymbol, fir d'Benotzeriwwerfläch ze starten.
5. Wann d'Applikatioun geluede gëtt, wielt **Weider**, fir mat der Installatioun vum Patch unzefänken.
6. Wielt um Bildschierm "Installatioun ofschléissen" d'Optioun **Ofschléissen**.

Fir de Fall, datt eng Iwwerprüfung vum Installatiounsbericht erfuerderlech ass, kuckt wgl. *Iwwerprüfung* op Säit 5.

En Neistart nom Ofschloss vun der Installatioun ass erfuerderlech.

Reparéieren

Am Fall vun engem Feeler kann de Client d'Reparatur vun der Installatioun unhand vun de follgenden Installatioun duerchféieren:

1. Mellt lech iwwer en Administrateurskont (z. B. sbsadmin) um System un.
2. Sicht de Patch, deen op de System erofgeluede gouf.
3. Réckelt de Patchinstallatiounsprogramm an den Dossier `C:\Illumina` (ass vun der Softwareaschränkungsrichtlinn ausgeholl).
4. Duebelklickt op d'Installatiounsprogrammsymbol, fir d'Benotzeriwwerfläch ze starten.
5. Den Installatiounsprogramm erkennt automatesch, ob d'Konfiguratiounsgeschier schonn ausgeféiert gouf, a stellt nei Optioune bereet:
   a. Änneren: Ausgegrot an net verfügbar
   b. Reparéieren: Reparéiert Feeler a bitt Optioune fir d'Neikonfiguratioun.
   c. Ewechhuelen: Desinstalléiert de Patch a setzt en op d'Standardkonfiguratioun zeréck (kuckt *Desinstallatioun* op Säit 5)
6. Wielt um Bildschierm "Installatioun ofschléissen" d'Optioun **Ofschléissen**.

Fir de Fall, datt eng Iwwerprüfung vum Installatiounsbericht erfuerderlech ass, kuckt wgl. *Iwwerprüfung op Säit 5*.

En Neistart nom Ofschloss vun der Installatioun ass erfuerderlech.

Desinstallatioun

D'Desinstallatioun vum Patch mécht déi un der Applikatiounshost-Konfiguratiounsdatei virgeholl Ännerunge réckgängeg.

1. Mellt lech iwwer en Administrateurskont (z. B. sbsadmin) um System un.
2. Sicht de Patch, deen op de System erofgeluede gouf.
3. Réckelt de Patchinstallatiounsprogramm an den Dossier `C:\Illumina` (ass vun der Softwareaschränkungsrichtlinn ausgeholl).
4. Duebelklickt op d'Installatiounsprogrammsymbol, fir d'Benotzeriwwerfläch ze starten.
5. Wielt **Ewechhuelen**, fir de Patch ze desinstalléieren an all Wäerter op d'Standardastellungen zeréckzesetzen.
6. Wielt **Ewechhuelen**, fir d'Optioun fir d'Desinstallatioun vum Patch ze bestätegen an all Wäerter op d'Standardastellungen zeréckzesetzen.

Dës Astellung mécht de System onsécher a setzt en dem Risiko vun Ugréff aus. Et gëtt dréngend empfuel, all technesch Auswierkungen, déi d'Optioun fir d'Ewechhuele vum Patch verursaachen, virun der Desinstallatioun ze behiewen.

7. Wielt um Bildschierm "Installatioun ofschléissen" d'Optioun **Ofschléissen**.

Fir de Fall, datt eng Iwwerprüfung vum Installatiounsbericht erfuerderlech ass, kuckt wgl. *Iwwerprüfung op Säit 5*.

En Neistart nom Ofschloss vun der Installatioun gëtt empfuel.

Iwwerprüfung

Fir de Fall, datt d'Installatioun iwwerpréift muss ginn, gouf eng Iwwerprüfungsdatei erstallt, déi en Datum- an Zäitstempel, déi installéiert Versioun vu Local Run Manager an aner Wäerter fir d'Schlësseliwwerprüfung enthält. Fir dës Datei ze kréien, went lech wgl. un techsupport@illumina.com.

Zousätzlech Empfielunge fir d'Risikoverréngerung a Sécherheet

De sécheren Asaz vun RUO-Instrumenter an DX-Medezinapparater hänkt vun de Sécherheetsniveauen of. Illumina empfielt dréngend, datt Instrumenter an Apparater am klengsten Netzwierk-Subnetz oder Sécherheetskontext zesumme mat vertrauenswierdegen Apparater bereetgestallt ginn. D'Verwendung vu

Firewallen an aneren Netzwierkrichtlinne fir d'Zougrëffsbeschränkung op aner an- an ausgoend Opriff ass staark unzeroden.

Mir empfielen ausserdeem:

- Aktivéiert Transport Layer Security (TLS) fir sécherzestellen, datt all apparatvermëttelt Kommunikatioun verschlësselt ass.
  - Fir Transport Layer Security (TLS) ze aktivéieren, kuckt wgl. am Handbuch fir d'Local-Run-Manager-Software.

Alternativ Optiounen

Wann d'Ausféierung vu Patchen aus iergendengem Grond net méiglech ass, verréngeren déi follgend manuell Methoden de Risiko:

- Desaktivéiert de Remotezougrëff op Local Run Manager, andeems Dir Windows-Firewallreegelen derbäisetzt, fir agoend Verbindungen op de Porten 80 a 443 ze blockéieren.
  Den MSI-Installer blockéiert automatesch agoend Remoteverbindungen an der Konfiguratioun vum Local-Run-Manager-Webserver. Eng manuell Risikoreduktioun, déi dat selwecht Resultat erziilt, besteet doran, eng Windows-Firewall-Konfiguratioun ze implementéieren, fir agoend Verbindungen zu `HTTP (TCP:80)` an `HTTPS (TLS, TCP:443)` ze blockéieren.
  No der Implementéierung kann nëmmen op deem Computer, op deem Local Run Manager installéiert ass, op Local Run Manager zougegraff ginn. Den Zougrëff op dëse Manager ass vun anere Computeren, déi mam deem selwechten Netzwierk verbonne sinn, net méi méiglech.

> Wann de Benotzerworkflow den Remotezougrëff op Local Run Manager ëmfaasst, funktionéiert dës Funktionalitéit net méi.

- Minimiséiert d'Zuel vun aneren Netzwierkapparater.
  D'Konfiguratioun vum Netzwierk zur Minimiséierung vun der Zuel vun aneren Netzwierkapparater, déi mam betraffenen Apparat kommunizéiere kënnen, verréngert d'Potenzial vun der Ausnotzung. Wat manner Verbindunge fir de System verfügbar sinn, wat manner Méiglechkeete fir den Zougrëff zur Verfügung stinn. Dat kann eng Récksprooch mat Äre lokalen Informationssécherheets- oder IT-Ressourcen erfuerderen.
- Huelt d'Instrument aus dem Netzwierk.
  Wa keng aner Optioun méiglech ass, besteet déi lescht Moossnam doran, den Apparat vollstänneg aus dem Netzwierk ewechzehuelen. Doduerch gëtt den Zougrëff op Illumina-Cloud/SaaS-Servicer, wéi z. B. Proactive a BaseSpace® Sequence Hub, esouwéi typesch genomesch Aarbechtsofleef fir d'Auslagere vun Daten desaktivéiert.
  Dat kann eng Récksprooch mat Äre lokalen Informationssécherheets- oder IT-Ressourcen erfuerderen.

Untersuchung vum potenziell net autoriséierten Zougréff

Déi follgend Schrëtt kënnen dem Operateur vum Instrument dobäi hëllefen, festzestellen, ob en net autoriséierte Benotzer op de System zougegraff huet:

1. Iwwerpréift déi ënner `C:\inetpub\logs\LogFiles\W3SVC1` gespäichert IIS-Protokoller op anormal Opriff.
   - Normal Opriff vu "Local Run Manager"-Webservere gi follgendermoossen ugewisen:

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

   - Anormal Opriff vum "Local Run Manager"-Webserver kënne beispillsweis follgendermoossen ugewise ginn:

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

2. Iwwerpréift den IIS-Protokoll op Unzeeche fir POST-Uploade vun Inhalter, déi keng Manifestdateie sinn. Déi follgend Opriff géifen zum Beispill op verdächteg Aktivitéiten hiweisen:

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

3. Wann eng Antivirus-/Antimalware-Applikatioun installéiert ass, iwwerpréift d'Softwareprotokoller op Unzeeche vun anormalem Verhalen.
4. Iwwerpréift d'Windows-Protokoller op Unzeeche vun anormale Feelermeldungen.
   Wann e Bedroungakteur Zougréff mat Administrateursrechter kréie géif, hätt hien d'Méiglechkeet, all lokal Instrumentprotokoller an -ereegnesser ze änneren an ze läschen.

Iwwerpréift, ob de System versicht huet, op Endpunkten zouzegräifen. Eng Lëscht mat den erwaarten ausgoende Verbindunge fannt Dir ënner Computerfirewall steieren.

Kontaktéiert bei Bedarf Illumina Technesch Ënnerstëtzung, fir Ënnerstëtzung ze kréien.

Versiounsverlaf

Dokument	Datum	Beschreiwung vun der Ännerung
Dokument- Nr. 200017330 v02	Abrëll 2022	Empfielung derbäigesat, de Patch unzewenden, wann d'Instrument net a Betrib ass. Instruktioun derbäigesat, datt no der Patchinstallatioun en Neistart vum Instrument erfuerderlech ass. D'Beschreiwung vum Revisiounsverlaf fir v01 gouf korrigéiert.
Dokument- Nr. 200017330 v01	Abrëll 2022	Dokumentstitel op LRM-Softwarepatch 1.0 Instruktiounsguide geännert. All Erwänung vu v1.0.1 gouf ewechgeholl. Abschnitt derbäigesat, an deem d'Untersuchung vum potenziell net autoriséierten Zougréff behandelt gëtt.
Dokument- Nr. 200017330 v00	Mäerz 2022	Éischtveréffentlechung.