LRM Software Patch 1.0

illumina®

Ghid de instrucțiuni

Introducere

Illumina® a luat cunoștință de o vulnerabilitate de securitate prezentă în software-ul Local Run Manager și a furnizat un patch software pentru a proteja împotriva exploatării de la distanță a acestei vulnerabilități.

Local Run Manager este o aplicație software de sine stătătoare și face parte din configurația implicită pe următoarele sisteme:

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

*A se utiliza la diagnosticarea in vitro.

Acest ghid se aplică instrumentelor Illumina listate mai sus și, de asemenea, computerelor din afara instrumentului care au instalată versiunea autonomă a Local Run Manager.

Vulnerabilitatea este una de tip executare neautentificată a comenzilor de la distanță (RCE - Unauthenticated Remote Command Execution) cu un scor CVSS neatenuat de 10,0 Critic, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Următorii pași pentru atenuare sunt necesari pe toate instrumentele enumerate mai sus, pentru a securiza împotriva posibilității ca un utilizator neautorizat să acceseze unul sau mai multe instrumente și să execute un atac prin acces de la distanță.

Dacă, din anumite motive, programul de instalare nu poate fi rulat, consultați secțiunea de atenuări suplimentare de la sfârșitul acestui document sau contactați techsupport@illumina.com pentru asistență suplimentară.

Vedeți Obținerea actualizării pentru Local Run Manager pentru opțiuni privind descărcarea sau solicitarea unei copii a patch-ului.

- **Patch-ul v1.0.0** — va actualiza configurația web Local Run Manager și va dezactiva accesul de la distanță la Internet Information Services (IIS).

Obținerea Local Run Manager Security Patch

Există patru (4) opțiuni pentru obținerea Local Run Manager Security Patch.

Opțiunea 1 – Descărcați direct pe instrument

Cel mai rapid mod de a obține actualizarea de securitate pentru Local Run Manager este să o descărcați de la site-ul web de găzduire direct pe instrument.

1. Descărcați programul de instalare a patch-ului de la linkul furnizat prin e-mailul securizat pe instrumentul dvs.
2. Transferați fișierul în folderul `C:\Illumina` de pe instrument.
3. Urmați instrucțiunile din *Aplicarea Local Run Manager Security Patch* la pagina 4.

Opțiunea 2 – Descărcați programul de instalare a patch-ului pe computer și transferați-l pe instrument prin intermediul unei unități USB/unui folder partajat.

Dacă nu puteți descărca patch-ul de securitate pe instrument, vă recomandăm să îl descărcați pe un computer separat și apoi să îl transferați pe instrument.

Verificați integritatea unității USB cu reprezentanții dvs. de securitate înainte de utilizare. (Recomandat)

1. Descărcați programul de instalare a patch-ului de la linkul furnizat prin e-mailul securizat pe computerul sau laptopul dvs.
2. Copiați programul de instalare a patch-ului descărcat pe unitatea USB sau într-un folder partajat de pe computer.
3. Pentru unitatea USB, conectați unitatea la instrument.
4. Copiați programul de instalare a patch-ului de pe unitatea USB sau din folderul partajat în folderul `C:\Illumina` de pe instrument.
5. Urmați instrucțiunile din *Aplicarea Local Run Manager Security Patch* la pagina 4.

Opțiunea 3 – Solicitați asistență tehnică

Un reprezentant al serviciului de asistență tehnică Illumina vă va îndruma în procesul de aplicare a patch-ului folosind una dintre următoarele metode:

- Autentificare la distanță pentru asistența tehnică

  Un reprezentant al serviciului de asistență tehnică va putea să acceseze analizorul de la distanță și să instaleze patch-ul în numele clientului.

  Sistemul trebuie să fie accesibil de la distanță. Dacă aveți întrebări, solicitați asistență reprezentantului IT local.

- Instrucțiuni ghidate
  Un reprezentant al serviciului de asistență tehnică vă va oferi instrucțiuni la telefon. Pentru asistență, contactați reprezentantul local al serviciului de asistență tehnică.

Opțiunea 4 – Comandați o unitate preconfigurată de la Illumina

Unitățile USB cu protecție la scriere pot fi comandate gratuit de către client. Pentru a comanda unitatea cu patch-ul instalat, contactați techsupport@illumina.com.

Ar putea exista întârzieri ale livrărilor sau ale stocurilor care ar putea afecta promptitudinea livrării. Pentru o protecție mai rapidă a sistemelor, se recomandă ferm ca sistemele să fie protejate prin metoda care oferă cea mai eficientă cale de rezolvare.

Aplicarea programului de instalare a Local Run Manager Security Patch v.1.0

Atunci când este executat, programul Illumina MSI (Microsoft Installer) va actualiza configurația serverului web Local Run Manager pentru a împiedica executarea oricărui conținut încărcat de utilizator și va bloca orice acces de la distanță la interfața web Local Run Manager, de la conexiunile de rețea LAN.

Pentru acei utilizatori care utilizează interfața web Local Run Manager pentru a accesa de la distanță instrumentele, acest flux de lucru va înceta să mai funcționeze după instalarea acestui patch. Illumina intenționează să restabilească mai târziu această funcție cu ajutorul soluției software permanente pentru această problemă. Dacă acest lucru provoacă o întrerupere a fluxurilor de lucru stabilite, vă rugăm să contactați techsupport@illumina.com pentru asistență suplimentară.

Programul de instalare MSI este aplicabil tuturor versiunilor de Local Run Manager și va determina automat soluția corectă în funcție de versiunea Local Run Manager instalată pe instrument/computer.

De asemenea, acest program de instalare MSI va crea un fișier de audit care va arăta că măsura de atenuare a fost implementată, împreună cu un marcaj de timp pentru a reflecta instalarea corectă.

Rularea programului de instalare MSI – la prima rulare a programului de instalare MSI, acesta va aplica patch-ul sistemului și va crea un fișier de audit cu ora de finalizare.

Repetarea rulării programului de instalare MSI va prezenta o opțiune **Repair (Reparare)**, utilizatorul având posibilitatea de a aplica din nou patch-ul sau de a-l anula. Notă: anularea patch-ului va duce la o configurație nesigură a instrumentului.

Aplicarea Local Run Manager Security Patch

Pentru a instala patch-ul:

1. Conectați-vă la sistem prin intermediul unui cont de administrator (de exemplu, sbsadmin).

   Illumina recomandă ca patch-ul să fie aplicat atunci când instrumentul nu rulează. Dacă instrumentul execută o secvență de rulare, patch-ul trebuie aplicat imediat după finalizarea secvenței de rulare.

2. Găsiți patch-ul care a fost descărcat în sistem.
3. Mutați programul de instalare a patch-ului în folderul `C:\Illumina` (exceptat de la politica de restricționare software).
4. Faceți dublu clic pe pictograma programului de instalare pentru a lansa interfața.
5. Când aplicația se încarcă, selectați „**Next**” (Următorul) pentru a începe instalarea patch-ului.
6. Pe ecranul Installation Completion (Finalizare instalare), selectați **Finish** (Finalizare).

Dacă este necesar un raport de verificare a instalării, consultați *Verificarea* la pagina 5.

Este necesară o repornire la sfârșitul instalării.

Repararea

În cazul unei erori, clientul poate executa repararea instalării urmând instrucțiunile de mai jos:

1. Conectați-vă la sistem prin intermediul unui cont de administrator (de exemplu, sbsadmin).
2. Găsiți patch-ul care a fost descărcat în sistem.
3. Mutați programul de instalare a patch-ului în folderul `C:\Illumina` (exceptat de la politica de restricționare software).
4. Faceți dublu clic pe pictograma programului de instalare pentru a lansa interfața.
5. Programul de instalare va detecta automat dacă instrumentul de configurare a fost executat anterior și va reprezenta noi opțiuni:
   a. Change (Modificare): gri și indisponibil
   b. Repair (Reparare): repară erorile și oferă opțiuni pentru reconfigurare.
   c. Remove (Eliminare): dezinstalează patch-ul și îl restabilește la configurația implicită (vedeți *Dezinstalarea* la pagina 5)
6. Pe ecranul Installation Completion (Finalizare instalare), selectați **Finish** (Finalizare).

Dacă este necesar un raport de verificare a instalării, consultați *Verificarea* la pagina 5.

Este necesară o repornire la sfârșitul instalării.

Dezinstalarea

Dezinstalarea patch-ului anulează modificările efectuate în fișierul de configurare pentru gazda aplicației.

1. Conectați-vă la sistem prin intermediul unui cont de administrator (de exemplu, sbsadmin).
2. Găsiți patch-ul care a fost descărcat în sistem.
3. Mutați programul de instalare a patch-ului în folderul `C:\Illumina` (exceptat de la politica de restricționare software).
4. Faceți dublu clic pe pictograma programului de instalare pentru a lansa interfața.
5. Selectați **Remove** (Eliminare) pentru a dezinstala patch-ul și a readuce toate valorile la setările implicite.
6. Selectați **Remove** (Eliminare) pentru a verifica opțiunea de dezinstalare a patch-ului și de readucere a tuturor valorilor la setările implicite.

> Această setare va face ca sistemul să fie nesigur și expus riscului de atac. Se recomandă ferm ca orice impact tehnic care determină opțiunea de a elimina patch-ul să fie abordat înainte de a alege dezinstalarea.

7. Pe ecranul Installation Completion (Finalizare instalare), selectați **Finish** (Finalizare).

> Dacă este necesar un raport de verificare a instalării, consultați *Verificarea* la pagina 5.

> Se recomandă o repornire la sfârșitul instalării.

Verificarea

Dacă este necesară verificarea instalării, va fi generat un fișier de verificare care include marcajul de dată și oră, versiunea de Local Run Manager instalată și alte valori cheie pentru verificare. Pentru a obține acest fișier, contactați techsupport@illumina.com.

Recomandări suplimentare privind atenuarea și securitatea

Implementarea în condiții de siguranță a instrumentelor RUO și a dispozitivelor medicale Dx depinde de nivelurile de securitate. Illumina recomandă cu tărie ca instrumentele și dispozitivele să fie implementate în cea mai mică subrețea de rețea sau cel mai mic context de securitate, cu dispozitive de încredere. Este ferm recomandată utilizarea unor firewalluri și a altor politici de rețea pentru a restricționa accesul de intrare și ieșire.

Recomandăm, de asemenea:

- Activați Transport Layer Security (TLS) pentru a vă asigura că toate comunicațiile în afara instrumentului sunt criptate.
  - Pentru a activa Transport Layer Security (TLS), consultați Ghidul software Local Run Manager.

Opțiuni alternative

Dacă, din anumite motive, executarea patch-ului nu este o opțiune, următoarele metode de atenuare manuală vor reduce riscul:

- Dezactivați accesul de la distanță la Local Run Manager prin adăugarea unor reguli de firewall Windows pentru a bloca conexiunile de intrare prin porturile 80 și 443.
  Programul de instalare MSI va bloca automat conexiunile de intrare de la distanță în configurația serverului web Local Run Manager. O măsură de atenuare manuală cu rezultat identic este implementarea unei configurații de firewall Windows pentru a bloca conexiunile de intrare către conexiunile `HTTP (TCP:80)` și `HTTPS (TLS, TCP:443).`
  După implementare, Local Run Manager va putea fi accesat numai de pe computerul pe care este instalat Local Run Manager; acesta nu va mai fi accesibil de pe alte computere conectate la aceeași rețea.

  Dacă fluxul de lucru pentru utilizatori implică accesarea de la distanță a Local Run Manager, această funcție nu va mai fi activă.

- Reduceți la minimum numărul celorlalte dispozitive de rețea.
  Configurarea rețelei pentru a minimiza numărul altor dispozitive de rețea care pot comunica cu instrumentul afectat va reduce potențialul unei exploatări. Cu cât sunt mai puține conexiuni disponibile la sistem, cu atât sunt mai puține oportunități disponibile de acces.
  Această măsură poate necesita consultarea cu resursele locale de securitate a informațiilor sau de IT pentru aplicare.
- Scoateți instrumentul din rețea.
  Dacă nu este fezabilă nicio altă opțiune, soluția finală de atenuare este de a elimina complet instrumentul din rețea. Aceasta va dezactiva accesul la serviciile Illumina Cloud/SaaS, cum ar fi Proactive și BaseSpace® Sequence Hub, precum și fluxurile de lucru de descărcare a datelor genomice tipice.
  Această măsură poate necesita consultarea cu resursele locale de securitate a informațiilor sau de IT pentru aplicare.

Investigarea potențialului acces neautorizat

Următorii pași ar putea ajuta operatorul instrumentului să determine dacă un utilizator neautorizat a accesat sistemul:

1. Examinați jurnalele IIS stocate în `C:\inetpub\logs\LogFiles\W3SVC1` pentru a detecta apelurile anormale.

- Apelurile normale către serverul web Local Run Manager arată ca mai jos:

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

- Apelurile anormale către serverul web Local Run Manager pot fi similare celui din exemplul de mai jos:

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

2. Examinați jurnalul IIS pentru a găsi indicii de încărcări de conținut POST, diferite de cele ale fișierelor manifest. De exemplu, următoarele apeluri pot indica o activitate suspectă:

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

3. Dacă este instalată o aplicație antivirus/antimalware, verificați jurnalele respectivului software pentru a vedea dacă există indicii de comportament anormal.
4. Examinați jurnalele Windows pentru a găsi indicii de mesaje de eroare anormale.
   Dacă un agent cauzator de amenințări obține acces cu drepturi de administrator, acesta ar avea capacitatea de a modifica sau de a șterge toate jurnalele și evenimentele locale ale instrumentului.

Verificați dacă există puncte finale pe care sistemul a încercat să le acceseze. Pentru o listă a conexiunilor de ieșire preconizate, consultați Control Computer Firewall (Controlarea firewallului computerului).

Contactați departamentul de Asistență tehnică Illumina pentru ajutor, dacă este necesar.

Istoricul reviziilor

Document	Data	Descrierea modificării
Nr. document 200017330 v02	Aprilie 2022	A fost adăugată recomandarea de a aplica patch-ul atunci când instrumentul nu rulează. A fost adăugată instrucțiunea că este necesară o repornire a instrumentului după instalarea patch-ului. A fost corectată descrierea istoricului revizuirilor pentru v01.
Nr. document 200017330 v01	Aprilie 2022	S-a modificat titlul documentului în LRM Software Patch 1.0 – Ghid de instrucțiuni. S-a eliminat orice mențiune la v1.0.1. A fost adăugată o secțiune care să acopere investigarea unui potențial acces neautorizat.
Nr. document 200017330 v00	Martie 2022	Versiunea inițială.

A SE UTILIZA LA DIAGNOSTICAREA IN VITRO

A se utiliza exclusiv în scop de cercetare. A nu se utiliza în cadrul procedurilor de diagnosticare.