Patch software 1.0 di LRM

illumina®

Manuale di istruzioni

Introduzione

Illumina® è venuta a conoscenza di una vulnerabilità di sicurezza presente nel software Local Run Manager e ha fornito una patch software per proteggere contro lo sfruttamento in remoto di questa vulnerabilità.

Local Run Manager è un'applicazione software indipendente e fa parte della configurazione predefinita sui seguenti sistemi:

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

* Per uso diagnostico in vitro.

La presente guida si applica agli strumenti Illumina sopra elencati ed anche agli strumenti installati su altri computer che hanno installata la versione indipendente di Local Run Manager.

La vulnerabilità è un Unauthenticated Remote Command Execution (RCE) con un punteggio CVSS non mitigato di 10,0, ossia Critico, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

La seguente procedura di mitigazione è richiesta su tutti gli strumenti sopra elencati per proteggere contro un possibile accesso da parte di un utente non autorizzato a uno o più strumenti e dall'esecuzione di un accesso in remoto.

Se per qualche motivo non è possibile eseguire l'installer, consultare la sezione contenente le ulteriori mitigazione alla fine di questo documento oppure contattare techsupport@illumina.com per ulteriore assistenza.

Vedere Come ottenere l'aggiornamento di Local Run Manager per informazioni su come scaricare o richiedere una copia della patch.

- **Patch v1.0.0**: aggiorna la configurazione Web di Local Run Manager e disabilita l'accesso remoto tramite Internet Information Services (IIS).

Come ottenere la patch di sicurezza per Local Run Manager

Per ottenere la patch di sicurezza per Local Run Manager sono disponibili quattro (4) opzioni.

Opzione 1: scaricarlo direttamente sullo strumento in uso

Il modo più veloce per ottenere l'aggiornamento di sicurezza di Local Run Manager è quello di scaricarlo direttamente dal sito Web host sullo strumento.

1. Scaricare l'installer della patch dal link fornito via e-mail sicura sullo strumento.
2. Trasferire il file nella cartella `C:\Illumina` sullo strumento.
3. Attenersi alle istruzioni contenute in *Applicazione della patch di sicurezza per Local Run Manager* a pagina 4.

Opzione 2: scaricare l'installer della patch sul computer e trasferirlo sullo strumento tramite unità USB/cartella condivisa

Se non è possibile scaricare la patch di sicurezza sullo strumento, si raccomanda di scaricare la patch su un computer diverso, quindi trasferire la patch nello strumento interessato.

Prima dell'utilizzo, verificare l'integrità dell'unità USB con i responsabili della sicurezza. (Raccomandato).

1. Scaricare l'installer della patch dal link fornito via e-mail sicura sul computer o sul laptop.
2. Copiare l'installer della patch scaricato su un'unità USB o su una cartella condivisa dal computer.
3. Per l'unità USB, collegare l'unità allo strumento.
4. Copiare l'installer della patch dall'unità USB o dalla cartella condivisa nella cartella `C:\Illumina` sullo strumento.
5. Attenersi alle istruzioni contenute in *Applicazione della patch di sicurezza per Local Run Manager* a pagina 4.

Opzione 3: richiesta di assistenza tecnica

Un rappresentante dell'Assistenza Tecnica Illumina vi guiderà per tutta la procedura relativa alla patch utilizzando uno dei seguenti metodi:

- Accesso remoto da parte dell'Assistenza Tecnica
  Un rappresentante dell'Assistenza Tecnica accederà in remoto all'analizzatore e installerà la patch per il cliente.

  Il sistema deve essere accessibile in remoto. Per qualsiasi domanda e richiesta di assistenza rivolgersi al responsabile informatico della propria sede.

- Istruzioni guidate
  Un rappresentante dell'Assistenza Tecnica fornisce istruzioni guidate al telefono. Per assistenza, contattare il rappresentante dell'Assistenza Tecnica locale.

Opzione 4: ordinare un'unità preconfigurata da Illumina

Le unità USB protette da scrittura possono essere ordinate dal cliente senza alcuna spesa. Per ordinare l'unità contenente la patch installata, contattare techsupport@illumina.com.

Potrebbero verificarsi dei ritardi nelle spedizioni o a causa di giacenza che potrebbero influire sulla tempestività della consegna. Per proteggere tempestivamente i sistemi, è vivamente raccomandato di proteggere i sistemi con il metodo che offre la patch di risoluzione più efficiente.

Applicazione dell'installer della patch di sicurezza v.1.0 per Local Run Manager

MSI (Microsoft Installer) Illumina, quando eseguito, aggiornerà la configurazione del server Web di Local Run Manager per impedire l'esecuzione di qualsiasi contenuto caricato dagli utenti e blocca tutti gli accessi remoti all'interfaccia Web di Local Run Manager dalle connessioni di rete LAN.

Se gli utenti utilizzano l'interfaccia Web di Local Run Manager per accedere agli strumenti in remoto, questo flusso di lavoro non funzionerà più dopo l'installazione di questa patch. Illumina ha intenzione di ripristinare in futuro questa funzionalità con la correzione permanente del software in relazione a questo problema. Se questo causa un'interruzione ai flussi di lavoro utilizzati, contattare techsupport@illumina.com per ulteriore assistenza.

L'installer MSI si applica a tutte le versioni di Local Run Manager e determina automaticamente la correzione rilevante in base alla versione di Local Run Manager installata sullo strumento/computer.

L'installer MSI crea inoltre un file di audit nel quale è indicata l'implementazione di questa mitigazione assieme a un timestamp che riflette la corretta installazione.

Esecuzione dell'installer MSI: la prima volta che viene eseguito l'installer MSI, l'installer installerà la patch sul sistema e creerà un file di audit con i tempi di completamento.

Quando l'installer MSI viene eseguito di nuovo viene visualizzata un'opzione **Repair** (Risoluzione di errori) che consente all'utente di riapplicare o ripristinare la patch. Nota: il ripristino della patch fornirà una configurazione dello strumento non sicura.

Applicazione della patch di sicurezza per Local Run Manager

Per installare la patch:

1. Accedere al sistema con un account di amministratore (ad esempio, sbsadmin).

   Illumina raccomanda di applicare la patch quando lo strumento non è in funzione. Se lo strumento sta elaborando una corsa, la patch deve essere applicata immediatamente dopo il termine della corsa.

2. Individuare la patch scaricata sul sistema.
3. Spostare l'installer della patch nella cartella `C:\Illumina` (libera da policy di restrizione software).
4. Fare doppio clic sull'icona dell'installer per lanciare l'interfaccia.
5. Quando l'applicazione è in fase di caricamento, selezionare **Next** (Avanti) per iniziare l'installazione della patch.
6. Nella schermata Installation Completion (Installazione completata), selezionare **Finish** (Termina).

Nel caso in cui sia richiesto il report di installazione, vedere *Verifica* a pagina 5.

Al termine dell'installazione è richiesto un riavvio.

Risoluzione di errori

In caso di errori durante l'installazione, il cliente può risolverli attenendosi alle seguenti istruzioni:

1. Accedere al sistema con un account di amministratore (ad esempio, sbsadmin).
2. Individuare la patch scaricata sul sistema.
3. Spostare l'installer della patch nella cartella `C:\Illumina` (libera da policy di restrizione software).
4. Fare doppio clic sull'icona dell'installer per lanciare l'interfaccia.
5. L'installer rileva automaticamente se lo strumento di configurazione è stato eseguito in precedenza e presenta nuove opzioni:
   a. Change (Modifica): disattivato e non disponibile.
   b. Repair (Risoluzione di errori): risolve gli errori e fornisce opzioni per la riconfigurazione.
   c. Remove (Rimuovi): disinstalla la patch e ripristina la configurazione predefinita (vedere *Disinstallazione* a pagina 5).
6. Nella schermata Installation Completion (Installazione completata), selezionare **Finish** (Termina).

Nel caso in cui sia richiesto il report di installazione, vedere *Verifica* a pagina 5.

Al termine dell'installazione è richiesto un riavvio.

Disinstallazione

La disinstallazione della patch annulla le modifiche eseguite al file di configurazione host dell'applicazione.

1. Accedere al sistema con l'account di amministratore (ad esempio, sbsadmin).
2. Individuare la patch scaricata sul sistema.
3. Spostare l'installer della patch nella cartella `C:\Illumina` (libera da policy di restrizione software).
4. Fare doppio clic sull'icona dell'installer per lanciare l'interfaccia.
5. Selezionare **Remove** (Rimuovi) per disinstallare la patch e ripristinare tutti i valori alla configurazione predefinita.
6. Selezionare **Remove** (Rimuovi) per verificare l'opzione per disinstallare la patch e ripristinare tutti i valori alla configurazione predefinita.

Questa impostazione renderà il sistema insicuro e a rischio di attacco. Se risulta necessario scegliere l'opzione di rimozione della patch per ragioni tecniche, si raccomanda vivamente di valutare il problema prima di eseguire la disinstallazione.

7. Nella schermata Installation Completion (Installazione completata), selezionare **Finish** (Termina).

Nel caso in cui sia richiesto il report di installazione, vedere *Verifica* a pagina 5.

Al termine dell'installazione è raccomandato un riavvio.

Verifica

Nel caso sia necessario verificare l'installazione, deve essere generato un file di verifica che include una data e un timestamp, la versione installata di Local Run Manager e altri valori di verifica importanti. Per ottenere questo file, contattare techsupport@illumina.com.

Ulteriori raccomandazioni su mitigazione e sicurezza

L'implementazione sicura degli strumenti RUO e dei dispositivi medici Dx dipende dai livelli di sicurezza. Illumina raccomanda vivamente di implementare gli strumenti e i dispositivi nel più piccolo subnet di rete o contesto di sicurezza, con dispositivi affidabili. È fortemente raccomandato l'utilizzo di firewall e altre politiche di rete per limitare altri accessi in entrata e uscita.

Si raccomanda inoltre di:

- Abilitare Transport Layer Security (TLS) per assicurare comunicazioni cifrate per tutti gli strumenti eseguiti su altro computer.
  - Per abilitare Transport Layer Security (TLS), fare riferimento a Local Run Manager Software Guide (Guida del software Local Run Manager).

Opzioni alternative

Se qualche motivo non è possibile eseguire la patch, ridurre i rischi attenendosi ai seguenti metodi di mitigazione:

- Disattivare l'accesso remoto a Local Run Manager aggiungendo regole firewall di Windows per bloccare le connessioni in entrata alle porte 80 e 443.
  L'installer MSI blocca automaticamente le connessioni remote in entrata nella configurazione del server Web di Local Run Manager. Una mitigazione manuale che consente di ottenere lo stesso risultato è quella di implementare una configurazione del firewall di Windows per bloccare le connessioni in entrata alle connessioni `HTTP (TCP:80)` e `HTTPS (TLS, TCP:443)`.
  Una volta implementata la mitigazione, si può accedere a Local Run Manager solo sul computer in cui è installato Local Run Manager; non sarà più possibile accedervi da altri computer connessi alla stessa rete.

  Se il flusso di lavoro dell'utente comprende l'accesso remoto a Local Run Manager, questa funzionalità non sarà più disponibile.

- Ridurre al minimo il numero di altri dispositivi sulla rete.
  La configurazione della rete per ridurre al minimo il numero di altri dispositivi sulla rete che comunicano con lo strumento interessato ne ridurrà il potenziale sfruttamento. Se vi sono meno connessioni disponibili al sistema, minore sarà la possibilità di accedervi.
  Per questo potrebbe essere necessario consultare i responsabili della sicurezza delle informazioni o del dipartimento informatico della propria sede.

- Rimuovere lo strumento dalla rete.
  Se non sono possibili altre opzioni, la mitigazione finale è quella di rimuovere completamente lo strumento dalla rete. Questo disabiliterà l'accesso ai servizi Cloud/SaaS Illumina come il servizio proattivo, BaseSpace® Sequence Hub e i tipici flussi di lavoro che utilizzano dati genomici scaricati.
  Per questo potrebbe essere necessario consultare i responsabili della sicurezza delle informazioni o del dipartimento informatico della propria sede.

Ricerca di potenziale accesso non autorizzato

La procedura seguente può aiutare l'operatore dello strumento nel determinare se un utente non autorizzato ha avuto accesso al sistema:

1. Esaminare i registri IIS archiviati in `C:\inetpub\logs\LogFiles\W3SVC1` per individuare accessi anomali.
   - I normali accessi al server Web Local Run Manager appaiono come segue:

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

- Quanto segue sono esempi di come possono apparire gli accessi anomali al server Web di Local Run Manager:

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

2. Esaminare i registri IIS per individuare caricamenti di contenuti POST che non siano i file manifest. Ad esempio, le seguenti attività potrebbero indicare attività sospetta:

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

3. Se è installata un'applicazione antivirus/antimalware, controllare che nei file di registro non siano presenti attività anomale.
4. Esaminare i registri di Windows per controllare la presenza di messaggi di errore anomali.
   Se un threat actor ha eseguito l'accesso con diritti di amministratore, questi potrebbe alterare o eliminare tutti i registri ed eventi locali dello strumento.

Controllare eventuali endpoint ai quali il sistema potrebbe aver tentato l'accesso. Per un elenco delle connessioni in uscita previste, fare riferimento a Firewall del computer di controllo.

Se necessario, contattare l'Assistenza Tecnica Illumina per assistenza.

Cronologia revisioni

Documento	Data	Descrizione della modifica
Documento n. 200017330 v02	Aprile 2022	Aggiunta la raccomandazione di applicare la patch quando lo strumento non è in funzione. Aggiunta l'istruzione indicante che, dopo l'installazione della patch, è richiesto un riavvio dello strumento. Corretta la descrizione della cronologia delle revisioni per v01.
Documento n. 200017330 v01	Aprile 2022	Cambiato il titolo del documento in Manuale di istruzioni per la patch software 1.0 di LRM. Rimosso qualsiasi riferimento a v1.0.1. Aggiunta la sezione che indica come cercare il potenziale accesso non autorizzato.
Documento n. 200017330 v00	Marzo 2022	Versione iniziale.