LRM Software Patch 1.0

illumina®

Anleitung

Einführung

Illumina® hat Kenntnis von einer Sicherheitslücke in der Local Run Manager-Software erhalten und einen Software-Patch bereitgestellt, der verhindert, dass die Sicherheitslücke per Fernzugriff ausgenutzt werden kann.

Local Run Manager ist eine eigenständige Softwareanwendung und Teil der Standardkonfiguration folgender Systeme:

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

* Für die In-vitro-Diagnostik.

Die vorliegende Anleitung bezieht sich auf die oben aufgeführten Illumina-Geräte sowie auf vom Gerät separate Computer, auf denen die eigenständige Version von Local Run Manager installiert ist.

Bei der Sicherheitslücke handelt es sich um die Ausführung von Remote-Befehlen (RCE, Remote Command Execution) ohne Authentifizierung. Der CVSS-Score ist 10,0 (kritisch) `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Die folgenden Abhilfemaßnahmen sind auf den oben aufgeführten Geräten erforderlich, um unbefugten Benutzerzugriff auf einem oder mehreren Geräte sowie die Durchführung von Remote-Angriffen zu verhindern.

Kann das Installationsprogramm aus irgendeinem Grund nicht ausgeführt werden, finden Sie im Abschnitt über zusätzliche Abhilfemaßnahmen am Ende dieses Dokuments weitere Informationen. Hilfe erhalten Sie ggf. per E-Mail an techsupport@illumina.com.

Unter Bezug des Updates für Local Run Manager erfahren Sie, wie Sie den Patch herunterladen oder anfordern können.

- **Patch v1.0.0**: aktualisiert die Webkonfiguration von Local Run Manager und deaktiviert den Remote-Zugriff auf Internet Information Services (IIS).

Bezug des Sicherheitspatches für Local Run Manager

Es stehen vier (4) Möglichkeiten zum Bezug des Sicherheitspatches für Local Run Manager zur Verfügung.

Option 1: Direkter Download auf Ihr Gerät

Am schnellsten erhalten Sie das Sicherheitsupdate für Local Run Manager, indem Sie es direkt von der Hosting-Website auf das Gerät herunterladen.

1. Laden Sie das Installationsprogramm für den Patch über den in der sicheren E-Mail bereitgestellten Link auf das Gerät herunter.
2. Kopieren Sie die Datei in den Ordner `C:\Illumina` auf dem Gerät.
3. Befolgen Sie die Anweisungen unter *Anwenden des Sicherheitspatches für Local Run Manager* auf Seite 4.

Option 2: Download des Installationsprogramms für den Patch auf den Computer und Übertragung mithilfe eines USB-Laufwerks/eines freigegebenen Ordners auf das Gerät

Wenn Sie den Sicherheits-Patch nicht auf das Gerät herunterladen können, empfehlen wir, diesen auf einen anderen Computer herunterzuladen und dann auf das Gerät zu übertragen.

Überprüfen Sie die Integrität des USB-Laufwerks vor der Verwendung gemeinsam mit einem für die Datensicherheit zuständigen Mitarbeiter. (Empfohlen)

1. Laden Sie das Installationsprogramm für den Patch über den in der sicheren E-Mail bereitgestellten Link auf Ihren Computer oder Laptop herunter.
2. Kopieren Sie das heruntergeladene Installationsprogramm für den Patch auf ein USB-Laufwerk oder in einen freigegebenen Ordner auf dem Computer.
3. Falls Sie ein USB-Laufwerk verwenden, schließen Sie es an das Gerät an.
4. Kopieren Sie das Installationsprogramm für den Patch vom USB-Laufwerk oder dem freigegebenen Ordner in den Ordner `C:\Illumina` auf dem Gerät.
5. Befolgen Sie die Anweisungen unter *Anwenden des Sicherheitspatches für Local Run Manager* auf Seite 4.

Option 3: Anfordern von technischem Support

Ein Mitarbeiter des technischen Supports von Illumina führt Sie mit einer der folgenden Methoden durch den Patching-Prozess:

- Remote-Anmeldung durch den technischen Support
  Ein Mitarbeiter des technischen Supports meldet sich per Remote-Zugriff auf dem Analysegerät an installiert den Patch für den Kunden.

  Der Remote-Zugriff auf das Gerät muss möglich sein. Wenden Sie sich bei Fragen an Ihre IT-Abteilung.

- Telefonische Unterstützung
  Ein Mitarbeiter des technischen Supports leitet Sie telefonisch an. Wenden Sie sich bitte an den zuständigen technischen Support.

Option 4: Bestellen eines vorkonfigurierten Laufwerks bei Illumina

Kunden können ein kostenloses schreibgeschütztes USB-Laufwerk bestellen. Wenden Sie sich an techsupport@illumina.com, wenn Sie ein Laufwerk mit dem installierten Patch bestellen möchten.

Wie zeitnah die Bereitstellung erfolgt, hängt vom Transportweg und dem verfügbaren Bestand ab. Zum möglichst unmittelbaren Schutz wird dringend empfohlen, die effizienteste Lösung zu verwenden.

Ausführen des Local Run Manager Security Patch v.1.0-Installationsprogramms

Durch die Ausführung des MSI (Microsoft-Installationsprogramm) von Illumina wird die Konfiguration des Local Run Manager-Webservers aktualisiert. Dadurch wird die Ausführung sämtlicher von Benutzern hochgeladener Inhalte verhindert und der Remote-Zugriff auf die Weboberfläche von Local Run Manager über LAN-Verbindungen blockiert.

Benutzer können die Weboberfläche von Local Run Manager nach der Installation dieses Patches nicht mehr für den Remote-Zugriff auf Geräte verwenden. Illumina beabsichtigt, diese Funktion zu einem späteren Zeitpunkt mit dem permanenten Software-Fix für dieses Problem wiederherzustellen. Wenn dies zu einer Unterbrechung der derzeitigen Workflows führt, wenden Sie sich bitte an techsupport@illumina.com. Sie erhalten dann weitere Unterstützung.

Das MSI-Installationsprogramm ist mit allen Versionen von Local Run Manager kompatibel und ermittelt den passenden Fix anhand der auf dem Gerät/Computer installierten Local Run Manager-Version automatisch.

Das MSI-Installationsprogramm erstellt zusätzlich eine Audit-Datei, die mit einem Zeitstempel die ordnungsgemäße Umsetzung der Abhilfemaßnahme dokumentiert.

Ausführen des MSI-Installationsprogramms: Bei der ersten Ausführung des MSI-Installationsprogramms wendet das Programm den System-Patch an und erstellt eine Audit-Datei, die den Zeitpunkt der Fertigstellung angibt.

Bei der erneuten Ausführung des MSI-Installationsprogramms wird die Option **Repair** (Reparieren) angezeigt, mit der der Benutzer den Patch erneut anwenden oder den Systemzustand vor der Anwendung wiederherstellen kann. Hinweis: Die Gerätekonfiguration ist nicht mehr sicher, wenn der Patch entfernt wird.

Anwenden des Sicherheitspatches für Local Run Manager

So installieren Sie den Patch:

1. Melden Sie sich über ein Administratorkonto (z. B. sbsadmin) beim System an.

   Illumina empfiehlt, den Patch anzuwenden, während das Gerät keinen Lauf durchführt. Wenn das Gerät gerade einen Lauf durchführt, sollte der Patch unmittelbar nach Abschluss des Laufs angewendet werden.

2. Rufen Sie den Ordner mit dem auf das System heruntergeladenen Patch auf.
3. Verschieben Sie das Installationsprogramm für den Patch in den Ordner `C:\Illumina` (von der Richtlinie für Softwareeinschränkung ausgenommen).
4. Doppelklicken Sie auf das Symbol für das Installationsprogramm, um dieses zu starten.
5. Wählen Sie, nachdem die Anwendung geladen wurde, **Next** (Weiter), um mit der Installation des Patches zu beginnen.
6. Wählen Sie auf dem Bildschirm „Installation Completion“ (Abschluss der Installation) die Option **Finish** (Fertigstellen).

Falls ein Bericht über die Verifizierung der Installation erforderlich ist, finden Sie unter *Verifizierung* auf Seite 5 weitere Informationen.

Nach Abschluss der Installation muss ein Neustart durchgeführt werden.

Reparieren

Im Falle eines Fehlers kann der Kunde die Installation mithilfe der nachstehenden Anweisungen reparieren:

1. Melden Sie sich über ein Administratorkonto (z. B. sbsadmin) beim System an.
2. Rufen Sie den Ordner mit dem auf das System heruntergeladenen Patch auf.
3. Verschieben Sie das Installationsprogramm für den Patch in den Ordner `C:\Illumina` (von der Richtlinie für Softwareeinschränkung ausgenommen).
4. Doppelklicken Sie auf das Symbol für das Installationsprogramm, um dieses zu starten.
5. Das Installationsprogramm erkennt automatisch, ob das Konfigurationsprogramm bereits ausgeführt wurde, und zeigt neue Optionen an:
   a. Change (Ändern): ausgegraut und nicht verfügbar
   b. Repair (Reparieren): behebt Fehler und bietet Optionen zur Neukonfiguration
   c. Remove (Entfernen): deinstalliert das Patch und stellt die Standardkonfiguration des Systems wieder her (siehe *Deinstallieren* auf Seite 5)

6. Wählen Sie auf dem Bildschirm „Installation Completion“ (Abschluss der Installation) die Option **Finish** (Fertigstellen).

Falls ein Bericht über die Verifizierung der Installation erforderlich ist, finden Sie unter *Verifizierung* auf Seite 5 weitere Informationen.

Nach Abschluss der Installation muss ein Neustart durchgeführt werden.

Deinstallieren

Die Deinstallation des Patches macht die an der Konfigurationsdatei des Anwendungshosts vorgenommenen Änderungen rückgängig.

1. Melden Sie sich über ein Administratorkonto (z. B. sbsadmin) beim System an.
2. Rufen Sie den Ordner mit dem auf das System heruntergeladenen Patch auf.
3. Verschieben Sie das Installationsprogramm für den Patch in den Ordner `C:\Illumina` (von der Richtlinie für Softwareeinschränkung ausgenommen).
4. Doppelklicken Sie auf das Symbol für das Installationsprogramm, um dieses zu starten.
5. Wählen Sie **Remove** (Entfernen), um das Patch zu deinstallieren und die Standardwerte wiederherzustellen.
6. Wählen Sie **Remove** (Entfernen), um zu prüfen, ob das Patch deinstalliert und die Standardeinstellungen wiederhergestellt werden können.

Dadurch wird das System unsicher und angreifbar. Es wird dringend empfohlen, den Patch nur zu deinstallierten, wenn sich die technischen Ursachen, die eine Deinstallation erforderlich machen, nicht beseitigen lassen.

7. Wählen Sie auf dem Bildschirm „Installation Completion“ (Abschluss der Installation) die Option **Finish** (Fertigstellen).

Falls ein Bericht über die Verifizierung der Installation erforderlich ist, finden Sie unter *Verifizierung* auf Seite 5 weitere Informationen.

Es wird empfohlen, nach Abschluss der Installation einen Neustart durchzuführen.

Verifizierung

Für den Fall, dass die Installation verifiziert werden muss, wird eine Verifizierungsdatei erstellt, die einen Datums- und Zeitstempel, die installierte Version von Local Run Manager und andere wichtige Verifizierungswerte enthält. Wenden Sie sich an techsupport@illumina.com, wenn Sie diese Datei benötigen.

Empfohlene zusätzliche Abhilfe- und Sicherheitsmaßnahmen

Die Sicherheit des Einsatzes von RUO-Geräten (Research Use Only, nur für Forschungszwecke) und Dx-Medizinprodukten (Diagnostics, Diagnose) beruht auf unterschiedlichen Sicherheitsebenen. Illumina empfiehlt dringend, Geräte und Produkte im kleinstmöglichen Netzwerksubnetz bzw. Sicherheitskontext mit vertrauenswürdigen Geräten einzusetzen. Ebenso wird die Verwendung von Firewalls und anderen Netzwerkrichtlinien zur Beschränkung des internen und externen Zugriffs empfohlen.

Weitere Empfehlungen:

- Aktivieren Sie Transport Layer Security (TLS), um sicherzustellen, dass die gesamte externe Gerätekommunikation verschlüsselt wird.
  - Informationen zur Aktivierung von Transport Layer Security (TLS) finden Sie im Softwarehandbuch zu Local Run Manager.

Alternative Optionen

Wenn die Ausführung des Patches nicht möglich ist, lässt sich das Risiko mit folgenden manuellen Methoden minimieren:

- Deaktivieren Sie den Remote-Zugriff auf Local Run Manager, indem Sie Windows-Firewall-Regeln einrichten, die eingehende Verbindungen über die Ports 80 und 443 blockieren.
  Das MSI-Installationsprogramm blockiert automatisch eingehende Remote-Verbindungen in der Webserver-Konfiguration von Local Run Manager. Eine manuelle Abhilfemaßnahme, mit der sich dasselbe Ergebnis erzielen lässt, ist die Blockierung eingehender Verbindungen an `HTTP (TCP:80)` und `HTTPS (TLS, TCP:443)` in der Konfiguration der Windows-Firewall.
  Anschließend kann auf Local Run Manager nur noch auf dem Computer zugegriffen werden, auf dem Local Run Manager installiert ist. Von anderen Computern im selben Netzwerk ist dies nicht mehr möglich.

  Wenn der Benutzer-Workflow einen Remote-Zugriff auf Local Run Manager umfasst, steht diese Funktion nicht mehr zur Verfügung.

- Minimieren Sie die Anzahl der anderen Geräte im Netzwerk.
  Je weniger Geräte sich im Netzwerk befinden, die mit dem betroffenen Gerät kommunizieren können, desto geringer ist die Angriffsfläche. Je weniger Verbindungen zum System vorhanden sind, desto weniger Zugangsmöglichkeiten gibt es.
  Möglicherweise muss diese Maßnahme in Abstimmung mit der zuständigen Informationssicherheits- oder IT-Abteilung erfolgen.

- Entfernen Sie das Gerät aus dem Netzwerk.
  Wenn keine der anderen Maßnahmen durchgeführt werden kann, besteht die letzte Abhilfemaßnahme darin, das Gerät vollständig aus dem Netzwerk zu entfernen. Dadurch können Cloud-/SaaS-Dienste von Illumina wie Proactive und BaseSpace® Sequence Hub sowie typische Workflows zur externen Speicherung genomischer Daten nicht mehr genutzt werden.
  Möglicherweise muss diese Maßnahme in Abstimmung mit der zuständigen Informationssicherheits- oder IT-Abteilung erfolgen.

Untersuchung eines möglichen unbefugten Zugriffs

Geräteanwender können mithilfe der folgenden Schritte ermitteln, ob ein unbefugter Benutzer auf das System zugegriffen hat:

1. Prüfen Sie die unter `C:\inetpub\logs\LogFiles\W3SVC1` gespeicherten IIS-Protokolle auf ungewöhnliche Aufrufe.
   - Normale Aufrufe an den Local Run Manager-Webserver sehen wie folgt aus:
     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```
   - Ungewöhnliche Aufrufe an den Local Run Manager-Webserver sehen beispielsweise wie folgt aus:
     ```
     POST http /hackertool.asp
     ```
2. Prüfen Sie das IIS-Protokoll auf Anzeichen von POST-Uploads von anderen Inhalten als Manifestdateien. Die folgenden Aufrufe deuten beispielsweise auf verdächtige Aktivitäten hin:
   ```
   wscript
   shell
   wscript.network
   scripting.filesystemObject
   ```
3. Wenn eine Antiviren-/Antimalware-Anwendung installiert ist, sollten Sie die Softwareprotokolle auf ungewöhnliches Verhalten prüfen.
4. Prüfen Sie die Windows-Protokolle auf Anzeichen ungewöhnlicher Fehlermeldungen.
   Wenn sich der Urheber einer Bedrohung Zugang mit Administratorrechten verschafft hat, kann er sämtliche lokale Geräteprotokolle und -ereignisse ändern bzw. löschen.

Überprüfen Sie, auf welche Endpunkte vom System aus möglicherweise zugegriffen wurde. Eine Liste der erwarteten ausgehenden Verbindungen finden Sie in Control Computer Firewall (Firewall auf dem Steuerungscomputer).

Wenden Sie sich bei Bedarf an den technischen Support von Illumina.

Versionshistorie

Dokument	Datum	Beschreibung der Änderung
Dokument-Nr. 200017330 v02	April 2022	Empfehlung hinzugefügt, den Patch anzuwenden, während das Gerät keinen Lauf durchführt. Hinweis hinzugefügt, dass nach der Installation des Patches ein Neustart des Geräts erforderlich ist. Beschreibung der Versionshistorie für v01 korrigiert.
Dokument-Nr. 200017330 v01	April 2022	Titel des Dokuments in „LRM Software Patch 1.0 Anleitung“ geändert. Alle Verweise auf v1.0.1 entfernt. Abschnitt „Untersuchung eines möglichen unbefugten Zugriffs“ hinzugefügt.
Dokument-Nr. 200017330 v00	März 2022	Erste Version.