Parche del software LRM 1.0

illumina®

Guía de instrucciones

Introducción

Illumina® ha tenido conocimiento de una vulnerabilidad de seguridad presente en el software Local Run Manager y ha proporcionado un parche de software para la protección contra la explotación remota de esta vulnerabilidad.

Local Run Manager es una aplicación de software independiente y forma parte de la configuración predeterminada de los siguientes sistemas:

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

*Para uso diagnóstico in vitro.

Esta guía se aplica a los instrumentos de Illumina enumerados anteriormente y a los ordenadores fuera del instrumento que tienen instalada la versión independiente de Local Run Manager en los mismos.

La vulnerabilidad es una Ejecución Remota de Comandos (RCE, Remote Command Execution) no autenticada con una puntuación CVSS no mitigada de 10,0, Crítico, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Los siguientes pasos de mitigación son necesarios en los instrumentos enumerados anteriormente para protegerse contra la posibilidad de que un usuario no autorizado obtenga acceso a uno o más instrumentos y ejecute un ataque de acceso remoto.

Si, por alguna razón, no se puede ejecutar el instalador, consulte la sección de mitigaciones adicionales al final de este documento o póngase en contacto enviando un correo electrónico a techsupport@illumina.com para obtener más ayuda.

Consulte Obtener la actualización de Local Run Manager para conocer las opciones sobre cómo descargar o solicitar una copia del parche.

- **Parche v1.0.0**: actualizará la configuración web de Local Run Manager y desactivará el acceso remoto a Internet Information Services (IIS).

Obtener el parche de seguridad de Local Run Manager

Existen cuatro (4) opciones para obtener el parche de seguridad de Local Run Manager.

Opción 1: descárguela directamente en su instrumento

La forma más rápida de obtener la actualización de seguridad de Local Run Manager es descargarla directamente del sitio web de alojamiento en el instrumento.

1. Descargue el instalador del parche desde el enlace proporcionado por correo electrónico seguro en su instrumento.
2. Transfiera el archivo a la carpeta `C:\Illumina` en el instrumento.
3. Siga las instrucciones de *Aplicar el parche de seguridad de Local Run Manager* en la página 4.

Opción 2: descargue el instalador del parche en el ordenador y transfiéralo al instrumento a través de la unidad USB/carpeta compartida

Si no puede descargar el parche de seguridad en el instrumento, le recomendamos que lo descargue en otro ordenador y, a continuación, lo transfiera al instrumento.

Verifique la integridad de la unidad USB con sus representantes de seguridad antes de su uso. (Recomendado)

1. Descargue el instalador del parche desde el enlace proporcionado por correo electrónico seguro en su ordenador o portátil.
2. Copie el instalador del parche descargado en la unidad USB o en la carpeta compartida del ordenador.
3. En el caso de la unidad USB, conecte la unidad al instrumento.
4. Copie el instalador del parche de la unidad USB o la carpeta compartida en la carpeta `C:\Illumina` en el instrumento.
5. Siga las instrucciones de *Aplicar el parche de seguridad de Local Run Manager* en la página 4.

Opción 3: solicite asistencia técnica

Un representante del servicio de asistencia técnica de Illumina le guiará en el proceso de aplicación de parches mediante uno de los siguientes métodos:

- Inicio de sesión en remoto del servicio de asistencia técnica
  Un representante del servicio de asistencia técnica accederá en remoto al analizador e instalará el parche en nombre del cliente.

  El sistema debe ser accesible en remoto. Si tiene alguna duda, póngase en contacto con su representante local de TI para obtener ayuda.

- Instrucciones guiadas
  Un representante del servicio de asistencia técnica le proporcionará instrucciones guiadas por teléfono. Póngase en contacto con su representante local del servicio de asistencia técnica para obtener ayuda.

Opción 4: solicite una unidad preconfigurada a Illumina

El cliente puede solicitar sin coste alguno unidades USB con protección contra escritura. Para solicitar la unidad con el parche instalado, póngase en contacto enviando un correo electrónico a techsupport@illumina.com.

Podría haber retrasos en los envíos o en el inventario que pueden afectar a la puntualidad de la entrega. Para proteger los sistemas de manera más inmediata, se recomienda encarecidamente proteger los sistemas mediante el método que ofrezca la vía de resolución más eficaz.

Aplicar el instalador del parche de seguridad de Local Run Manager v.1.0

MSI (Microsoft Installer) de Illumina, cuando se ejecute, actualizará la configuración del servidor web de Local Run Manager para impedir la ejecución de cualquier contenido cargado por el usuario y bloqueará todo acceso remoto a la interfaz web de Local Run Manager desde las conexiones de la red LAN.

Para aquellos usuarios que usan la interfaz web de Local Run Manager para el acceso remoto a los instrumentos, este flujo de trabajo dejará de funcionar tras la instalación de este parche. Illumina tiene previsto restablecer esta funcionalidad con la corrección permanente del software para este problema más adelante. Si esto provoca una interrupción de los flujos de trabajo establecidos, póngase en contacto enviando un correo electrónico a techsupport@illumina.com para obtener más ayuda.

El instalador MSI es aplicable a todas las versiones de Local Run Manager y determinará automáticamente la corrección necesaria en función de la versión de Local Run Manager instalada en el instrumento/ordenador.

Este instalador MSI también creará un archivo de auditoría que muestra que esta mitigación se implementó junto con una marca de tiempo para reflejar la instalación adecuada.

Ejecución del instalador MSI: cuando se ejecute el instalador MSI por primera vez, este aplicará parches en el sistema y creará un archivo de auditoría con la hora de finalización.

Si se ejecuta de nuevo el instalador MSI, aparecerá la opción **Repair** (Reparación), en la que el usuario tiene la opción de volver a aplicar o revertir el parche. Nota: La reversión del parche dará lugar a una configuración poco segura del instrumento.

Aplicar el parche de seguridad de Local Run Manager

Para instalar el parche:

1. Acceda al sistema a través de una cuenta de administrador (por ejemplo, sbsadmin).

   Illumina recomienda que el parche se aplique cuando el instrumento no esté en funcionamiento. Si el instrumento está ejecutando un experimento, el parche debe aplicarse inmediatamente después de que se complete el experimento.

2. Localice el parche que se descargó en el sistema.
3. Desplace el instalador del parche a la carpeta `C:\Illumina` (exenta de la política de restricción de software).
4. Haga doble clic en el icono del instalador para iniciar la interfaz.
5. Cuando se cargue la aplicación, seleccione **Next** (Siguiente) para comenzar la instalación del parche.
6. En la pantalla Installation Completion (Finalización de la instalación), seleccione **Finish** (Finalizar).

En caso de que se requiera un informe de verificación de la instalación, consulte *Verificación* en la página 5.

Se necesita un reinicio al final de la instalación.

Reparación

En caso de error, el cliente puede ejecutar la reparación de la instalación siguiendo las siguientes instrucciones:

1. Acceda al sistema a través de una cuenta de administrador (por ejemplo, sbsadmin).
2. Localice el parche que se descargó en el sistema.
3. Desplace el instalador del parche a la carpeta `C:\Illumina` (exenta de la política de restricción de software).
4. Haga doble clic en el icono del instalador para iniciar la interfaz.
5. El instalador detectará automáticamente si la herramienta de configuración se ha ejecutado antes y presentará nuevas opciones:
   a. Cambiar: aparece en gris y no disponible
   b. Reparar: repara los errores y ofrece opciones de reconfiguración.
   c. Eliminar: desinstala el parche y restablece la configuración predeterminada (consulte *Desinstalación* en la página 5)
6. En la pantalla Installation Completion (Finalización de la instalación), seleccione **Finish** (Finalizar).

En caso de que se requiera un informe de verificación de la instalación, consulte *Verificación* en la página 5.

Se necesita un reinicio al final de la instalación.

Desinstalación

La desinstalación del parche revierte las modificaciones realizadas en el archivo de configuración del host de la aplicación.

1. Acceda al sistema a través de una cuenta de administrador (por ejemplo, sbsadmin).
2. Localice el parche que se descargó en el sistema.
3. Desplace el instalador del parche a la carpeta `C:\Illumina` (exenta de la política de restricción de software).
4. Haga doble clic en el icono del instalador para iniciar la interfaz.
5. Seleccione **Remove** (Eliminar) para desinstalar el parche y revertir todos los valores a la configuración predeterminada.
6. Seleccione **Remove** (Eliminar) para verificar la opción de desinstalar el parche y revertir todos los valores a la configuración predeterminada.

Esta configuración hará que el sistema sea poco seguro y corra el riesgo de ser atacado. Se recomienda encarecidamente que se aborden las posibles repercusiones técnicas que provoquen la opción de eliminar el parche antes de optar por la desinstalación.

7. En la pantalla Installation Completion (Finalización de la instalación), seleccione **Finish** (Finalizar).

En caso de que se requiera un informe de verificación de la instalación, consulte *Verificación* en la página 5.

Se recomienda un reinicio al final de la instalación.

Verificación

Si es necesario verificar la instalación, se generará un archivo de verificación que incluya una marca de fecha y hora, la versión de Local Run Manager instalada y otros valores clave de verificación. Para obtener este archivo, póngase en contacto enviando un correo electrónico a techsupport@illumina.com.

Recomendaciones adicionales de mitigación y seguridad

La instalación segura de los instrumentos RUO (Research Use Only) y los dispositivos médicos Dx (Diagnostic) depende de las capas de seguridad. Illumina recomienda encarecidamente que los instrumentos y dispositivos se instalen en la subred de la red o el contexto de seguridad más pequeños, con dispositivos de confianza. Es muy recomendable el uso de cortafuegos y otras políticas de red para restringir otros accesos de entrada y de salida.

También se recomienda:

- Activar la seguridad de la capa de transporte (TLS, Transport Layer Security) para garantizar que todas las comunicaciones fuera del instrumento estén cifradas.
  - Para activar la seguridad de la capa de transporte (TLS), consulte la Guía del software Local Run Manager.

Opciones alternativas

Si, por alguna razón, la ejecución del parche no es una opción, los siguientes métodos manuales de mitigación reducirán el riesgo:

- Desactivar el acceso remoto a Local Run Manager añadiendo reglas de cortafuegos de Windows para bloquear las conexiones entrantes de los puertos 80 y 443.
  El instalador MSI bloqueará automáticamente las conexiones remotas entrantes en la configuración del servidor web de Local Run Manager. Una mitigación manual que logra el mismo resultado consiste en la implementación de una configuración de cortafuegos de Windows para bloquear las conexiones entrantes a las conexiones `HTTP (TCP:80)` y `HTTPS (TLS, TCP:443)`.
  Una vez se implemente, solo se podrá acceder a Local Run Manager en el ordenador en el que esté instalado; ya no será accesible desde otros ordenadores conectados a la misma red.

> Si el flujo de trabajo del usuario implica el acceso remoto a Local Run Manager, esta funcionalidad dejará de funcionar.

- Minimizar el número de otros dispositivos de red.
  La configuración de la red para minimizar el número de otros dispositivos de red que se pueden comunicar con el instrumento afectado reducirá la posibilidad de explotación. Cuantas menos conexiones haya en el sistema, menos oportunidades de acceso habrá.
  Esto puede requerir la consulta de los recursos locales de seguridad de la información o de TI para su ejecución.

- Eliminar el instrumento de la red.
  Si no es factible ninguna otra opción, la última mitigación consiste en la eliminación del instrumento de la red por completo. Esto desactivará el acceso a los servicios de Illumina Cloud/SaaS, como Proactive y BaseSpace® Sequence Hub, y a los flujos de trabajo de descarga de datos genómicos típicos.
  Esto puede requerir la consulta de los recursos locales de seguridad de la información o de TI para su ejecución.

Investigación de posibles accesos no autorizados

Los siguientes pasos pueden ayudar al operador del instrumento a determinar si un usuario no autorizado ha obtenido acceso al sistema:

1. Examine los registros de IIS almacenados en `C:\inetpub\logs\LogFiles\W3SVC1` en busca de llamadas extrañas.
   - Las llamadas normales al servidor web de Local Run Manager aparecen de la siguiente manera:
     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```
   - Las llamadas extrañas al servidor web de Local Run Manager pueden aparecen, a modo de ejemplo, de la siguiente manera:
     ```
     POST http /hackertool.asp
     ```
2. Examine el registro de IIS en busca de señales de cargas POST de contenido que no sean archivos de manifiesto. Por ejemplo, las siguientes llamadas podrían indicar una actividad sospechosa:
   ```
   wscript
   shell
   wscript.network
   scripting.filesystemObject
   ```
3. Si está instalada una aplicación antivirus/antimalware, compruebe los registros del software en busca de signos de comportamiento extraño.
4. Examine los registros de Windows en busca de signos de mensajes de error extraños.
   Si un actor de amenazas lograra acceder con derechos de administrador, tendría la capacidad de alterar o borrar todos los registros y eventos de los instrumentos locales.

Compruebe si el sistema ha intentado acceder a algún punto de conexión. Para ver una lista de las conexiones de salida esperadas, consulte Cortafuegos del ordenador de control.

Póngase en contacto con el servicio de asistencia técnica de Illumina para obtener la ayuda necesaria.

Historial de revisiones

Documento	Fecha	Descripción del cambio
N.º de documento 200017330 v02	Abril de 2022	Se ha añadido la recomendación de aplicar el parche cuando el instrumento no está en funcionamiento. Se ha añadido la instrucción de que se necesita un reinicio del instrumento después de la instalación del parche. Se ha corregido la descripción del historial de revisiones de v01.
N.º de documento 200017330 v01	Abril de 2022	Se ha cambiado el título del documento a Guía de instrucciones del parche del software LRM 1.0 Se ha eliminado toda mención a v1.0.1. Se ha añadido una sección para abarcar la investigación de posibles accesos no autorizados.
N.º de documento 200017330 v00	Marzo de 2022	Publicación inicial.