LRM Software Patch 1.0

illumina®

Instruction Guide

Introduction

Illumina® has become aware of a security vulnerability present in Local Run Manager software and provided a software patch to protect against the remote exploitation of this vulnerability.

Local Run Manager is a standalone software application and part of the default configuration on the following systems:

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

*For in vitro diagnostic use.

This guide applies to the Illumina instruments listed above and also to off-instrument computers that have the standalone version of Local Run Manager installed on them.

The vulnerability is an Unauthenticated Remote Command Execution (RCE) with an unmitigated CVSS score of 10.0 Critical, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

The following mitigation steps are required on the instruments listed above to secure against the possibility of an unauthorized user accessing one or more instruments and executing a remote access attack.

If for some reason the installer cannot be run, consult the additional mitigations section at the end of this document, or contact techsupport@illumina.com for additional assistance.

See Obtain the Local Run Manager Update for options on how to download or request a copy of the patch.

- **v1.0.0 patch** - will update Local Run Manager web configuration and disable remote Internet Information Services (IIS) access.

Obtain the Local Run Manager Security Patch

There are four (4) options for obtaining the Local Run Manager Security Patch.

Option 1—Download directly to your instrument

The fastest way to obtain the Local Run Manager Security Update is to download it directly from the hosting website to the instrument.

1. Download the patch installer from the link provided via secure email to your instrument.
2. Transfer the file to `C:\Illumina` folder on the instrument.
3. Follow the instructions in *Apply the Local Run Manager Security Patch* on page 3.

Option 2—Download the patch installer to the computer and transfer it to the instrument via USB drive/shared folder

> ℹ If you cannot download the security patch to the instrument, we recommend downloading it to a separate computer and then transferring it to the instrument.

Verify the integrity of the USB drive with your Security representatives prior to use. (Recommended)

1. Download the patch installer from the link provided via secure email to your computer or laptop.
2. Copy downloaded patch installer to the USB drive or shared folder from the computer.
3. For USB drive, plug-in the drive into the Instrument.
4. Copy the patch installer from the USB drive or the shared folder to the `C:\Illumina` folder on the instrument.
5. Follow the instructions in *Apply the Local Run Manager Security Patch* on page 3.

Option 3—Request Technical Support

An Illumina Technical Support representative will guide you through the patching process using one of the following methods:

- Tech Support Remote login

  A Tech Support representative will access the analyzer remotely and install the patch on behalf of the customer.

  > ℹ The system must be remotely accessible. If you have any questions, ask your local IT representative for assistance.

- Guided Instructions

  A Tech Support representative will provide guided instruction over the phone. Please contact your local Tech Support representative for assistance.

Option 4—Order a preconfigured drive from Illumina

A write-protected USB drives can be ordered by the customer at no charge. To order the drive with patch installed, please contact techsupport@illumina.com.

ℹ There could be delays to shipments or inventory that may affect the timeliness of the delivery. To protect systems more immediately, it is highly recommended that systems be protected by the method that will offer the most efficient resolution path.

Apply the Local Run Manager Security Patch v.1.0 Installer

The Illumina MSI (Microsoft Installer), when executed, will update the Local Run Manager web server configuration to prevent the execution of any user uploaded content and block all remote access to the Local Run Manager web interface from LAN network connections.

For those users who use the Local Run Manager web interface to remotely access instruments, this workflow will cease to function after the installation of this patch. Illumina intends to restore this functionality with the permanent software fix for this issue later. If this causes an interruption to established workflows, please contact techsupport@illumina.com for further assistance.

The MSI installer is applicable to all versions of Local Run Manager and will automatically determine the correct fix based on the Local Run Manager version installed on the instrument/computer.

This MSI installer will also create an audit file showing that this mitigation was implemented along with a timestamp to reflect proper installation.

Running the MSI Installer – the first time the MSI Installer is run, the installer will patch the system and create an audit file with the completion time.

ℹ Running the MSI Installer again will present a **Repair** option, user is given the option to reapply or roll back the patch. Note: Rolling back the patch will result in an insecure instrument configuration.

Apply the Local Run Manager Security Patch

To install the patch:

1. Log into the system via an administrator account (eg, sbsadmin).

> Illumina recommends that the patch be applied when the instrument is not running. If the instrument is executing a run, the patch should be applied immediately after the run completes.

2. Locate the patch that was downloaded to the system.
3. Move the patch installer to the `C:\Illumina` folder (exempt from Software Restriction Policy).
4. Double-click on the installer icon to launch the interface.
5. When the application loads, select 'Next' to begin the installation of the patch.
6. At the Installation Completion screen, select 'Finish'.

> In the event a verification of installation report is required, please see *Verification* on page 5.

> A reboot at the end of installation is required.

Repair

In the event of an error, the customer can execute the repair of the installation by following the instructions below:

1. Log into the system via an administrator account (eg, sbsadmin).
2. Locate the patch that was downloaded to the system.
3. Move the patch installer to the `C:\Illumina` folder (exempt from Software Restriction Policy).
4. Double-click on the installer icon to launch the interface.
5. The installer will automatically detect if the configuration tool has been executed before and represent new options:
   a. Change: Grayed out and not available
   b. Repair: Repairs errors and gives options for reconfiguration.
   c. Remove: Uninstalls the patch and restores it to default configuration (see *Uninstallation* on page 4)
6. At the Installation Completion screen, select **Finish**.

> In the event a verification of installation report is required, please see *Verification* on page 5.

> A reboot at the end of installation is required.

Uninstallation

Uninstallation of the patch reverts the modifications made to the application host configuration file.

1. Log into the system via an administrator account (eg sbsadmin).
2. Locate the patch that was downloaded to the system.
3. Move the patch installer to the `C:\Illumina` folder (exempt from Software Restriction Policy).
4. Double-click on the installer icon to launch the interface.
5. Select **Remove** to uninstall the patch and revert all values to default settings.
6. Select **Remove** to verify the option to uninstall the patch and revert all values to default settings.

This setting will render the system as insecure and at risk of attack. It is highly recommended that any technical impacts that cause the option to remove the patch be addressed before choosing to uninstall.

7. At the Installation Completion screen, select **Finish**.

In the event a verification of installation report is required, please see *Verification* on page 5.

A reboot at the end of installation is recommended.

Verification

If there is a need to verify installation, a verification file will have been generated that includes a date and time stamp, version of Local Run Manager installed, and other key verification values. To obtain this file, please contact techsupport@illumina.com.

Additional Mitigation and Security Recommendations

Secure deployment of RUO instruments and Dx medical devices depends on layers of security. Illumina strongly recommends that instruments and devices are deployed in the smallest network subnet or security context, with trusted devices. Use of firewalls and other network policies to restrict other inbound and outbound access are highly advisable.

We also recommend:

- Enable Transport Layer Security (TLS) to ensure that all off-instrument communications are encrypted.
  - To enable Transport Layer Security (TLS), please refer to the Local Run Manager Software Guide.

Alternative Options

If for some reason executing the patch is not an option, the following manual mitigation methods will reduce the risk:

- Disable remote access to Local Run Manager by adding Windows firewall rules to block incoming Port 80 and 443 connections.
  The MSI Installer will automatically block remote incoming connections in the Local Run Manager web server configuration. A manual mitigation that achieves the same result is to implement a Windows firewall configuration to block incoming connections to `HTTP (TCP:80)` and `HTTPS (TLS, TCP:443)` connections.
  Once implemented, Local Run Manager can only be accessed on the computer that Local Run Manager is installed on; it will no longer be accessible from other computers connected to the same network.

ℹ If the user workflow involves remotely accessing Local Run Manager this functionality will no longer work.

- Minimize the number of other network devices.

  Configuring the network to minimize the number of other network devices that can communicate with the affected instrument will reduce the potential for exploitation. The fewer connections available to the system, the fewer opportunities available for access.

  This may require consultation with your local Information Security or IT resources to execute.

- Remove the instrument from the network.

  If no other option is feasible, the final mitigation is to remove the instrument from the network entirely. This will disable access to Illumina Cloud/SaaS services such as Proactive and BaseSpace® Sequence Hub, and typical genomic data offload workflows.

  This may require consultation with your local Information Security or IT resources to execute.

Investigation of Potential Unauthorized Access

The following steps might assist the instrument operator in determining whether an unauthorized user has accessed the system:

1. Examine the IIS logs stored in `C:\inetpub\logs\LogFiles\W3SVC1` for abnormal calls.
   - Normal calls to the Local Run Manager web server appears as follows:

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

   - Abnormal calls to the Local Run Manager web server may appear, as an example, as follows:

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

2. Examine the IIS log for signs of POST uploads of content other than manifest files. For example, the following calls would indicate suspicious activity:

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

3. If an anti-virus/anti-malware application is installed, check the software logs for signs of abnormal behavior.
4. Examine the windows logs for signs of abnormal error messages.

   If a threat actor achieved access with administrator rights, they would have the capability to alter or delete all local instrument logs and events.

Check for any endpoints that the system might have attempted to access. For a list of expected outbound connections, refer to Control Computer Firewall.

Contact Illumina Technical Support for assistance as required.

Revision History

Document	Date	Description of Change
Document # 200017330 v02	April 2022	Added recommendation to apply patch when the instrument is not running. Added instruction that a reboot of the instrument is required after patch installation. Corrected the revision history description for v01.
Document # 200017330 v01	April 2022	Changed document title to LRM Software Patch 1.0 Instruction Guide. Removed any mention of v1.0.1. Added section to cover the investigation of potential unauthorized access.
Document # 200017330 v00	March 2022	Initial release.

The instructions in this document must be strictly and explicitly followed by qualified and properly trained personnel in order to ensure the proper and safe use of the product(s) described herein. All of the contents of this document must be fully read and understood prior to using such product(s).

FAILURE TO COMPLETELY READ AND EXPLICITLY FOLLOW ALL OF THE INSTRUCTIONS CONTAINED HEREIN MAY RESULT IN DAMAGE TO THE PRODUCT(S), INJURY TO PERSONS, INCLUDING TO USERS OR OTHERS, AND DAMAGE TO OTHER PROPERTY, AND WILL VOID ANY WARRANTY APPLICABLE TO THE PRODUCT(S).

ILLUMINA DOES NOT ASSUME ANY LIABILITY ARISING OUT OF THE IMPROPER USE OF THE PRODUCT(S) DESCRIBED HEREIN (INCLUDING PARTS THEREOF OR SOFTWARE).