Recall

illumina

Wednesday, May 4, 2022

Quality Notification

URGENT MEDICAL DEVICE RECALL

Dear Customer,

Illumina is contacting you regarding a Local Run Manager (LRM) cybersecurity vulnerability that was identified in the NextSeq™ 550Dx and MiSeq™Dx instruments. This notice outlines the issue summary, Illumina actions, and required customer actions.

Table 1: Affected Product(s)

Product/Device Name	Device Identifier Number	Catalog Number
NextSeq 550Dx Instrument	00816270020125	20005715
MiSeqDx Instrument	00816270020002 / 00816270020699	DX-410-1001 / 15036706 / 20014053

Issue Summary

Illumina has identified a cybersecurity vulnerability affecting the Local Run Manager (LRM) software in the Illumina *in vitro* diagnostic (IVD) sequencing instruments identified in Table 1.

At this time, Illumina has not received any reports indicating this vulnerability has been exploited.

An unauthorized user could potentially exploit the vulnerability to take control of the instrument remotely and then take any action at the operating system level, including actions that could impact settings, configurations, software, or data on the instrument or a customer's network. Exploitation of this vulnerability could lead to the instrument producing no results, incorrect results, file corruption or a patient data breach. Exploitation of the vulnerability in such a manner could present a possible patient health risk.

Illumina Actions

Illumina has developed a software patch to protect against the exploitation of this vulnerability. We are actively working to provide a permanent software fix for current and future instruments.

For instruments connected to the internet, the software patch is available for immediate download (see Required Customer Actions section below for the website address). Illumina recommends that customers immediately download the software patch and install it to all your impacted instrument(s).

Technical Support:
techsupport@illumina.com

Customer Care:
customercare@illumina.com

For affected LRM products not connected to the internet, Illumina has developed other options for the installation of the software patch. Please contact Tech Support promptly at techsupport@illumina.com to obtain information about those options.

The pertinent local and international regulatory bodies, including the Competent Authorities, are being notified of this issue.

For any other questions or assistance, please contact techsupport@illumina.com.

Required Customer Actions

Note: The affected instruments have a dual boot mode, and it is important to install the software patch separately in each mode (Dx mode and RUO mode) of each instrument. It is also important to install the software patch to any stand-alone instances of the off-instrument LRM for RUO mode on the Dx instruments.

1. **For Each Instrument Connected to the Internet**: Immediately download and install the software patch, available here, in each mode (Dx mode and RUO mode) of each and every affected instrument and/or in each stand-alone instance of the off-instrument LRM for RUO mode on the Dx instruments.

   Before installing the software patch, we recommend that you back up your data.

   For your protection, Illumina is currently providing the website address only to impacted customers and regulatory authorities.

   Complete and return the Verification Form below within 5 business days.

2. **For Each Instrument Not Connected to the Internet**: Contact techsupport@illumina.com for instructions about other ways to implement the software patch.

   Complete and return the Verification Form below immediately after installing the software patch.

3. **Permanent Software Fix**: When it becomes available, install the software update that will permanently fix this vulnerability. We will send a separate communication with follow up information on this software update.

NOTE: Installation of the software patch will block remote access to the LRM web User Interface (web UI), superseding the current LRM user guide; the instrument will otherwise retain its essential

functions. For customers that depend on the web UI for laboratory workflows, please contact techsupport@illumina.com immediately for assistance.

NOTE: If you suspect your instrument may have been compromised by an unauthorized user, please immediately unplug the network cable and contact techsupport@illumina.com. Refer to the LRM Software Patch 1.0 Instruction Guide for steps to examine your device.

If you experience an adverse event due to this vulnerability with the use of the affected products, please report it to the FDA's MedWatch Adverse Event Reporting program either online, by regular mail or by fax. You can complete and submit the report online at www.fda.gov/medwatch/report.htm. In regions outside the USA, please contact your local regulatory authority.

Illumina takes data privacy and security issues very seriously. We are committed to supporting you in addressing this vulnerability. If you have any questions, email techsupport@illumina.com.

Sincerely,

Gary Workman

Electronically signed by: Gary Workman
Reason: Approver
Date: Apr 26, 2022 08:50 EDT

Gary Workman
VP, Global Quality

Karen Gutekunst

Electronically signed by: Karen Gutekunst
Reason: Approver
Date: Apr 26, 2022 08:37 PDT

Karen Gutekunst
VP, Regulatory Affairs

Why You're Receiving This Notification

We are sending this notification to you because our records indicate that you are one of the appropriate contacts for your organization. We occasionally need to inform our customers of product changes, product obsolescence, or quality issues.

Accordingly, please note that these notifications contain important information about our products and are not marketing communications. You may, therefore, receive these notifications even if you have opted out of receiving marketing material from Illumina. If you are not the appropriate individual in your organization to receive these types of notifications, please email customernotifications@illumina.com with the appropriate contact. For more information, please see our Privacy Policy.

illumina®

Verification Form

Dear Customer,

On May 4, 2022, Illumina sent you an Urgent Medical Device Recall Notice FSN2022-1230 regarding an issue affecting the NextSeq 550Dx and MiSeqDx instruments.

Please complete the table below to confirm that you received the notice. We ask that you kindly email the completed form to techsupport@illumina.com upon completion of the software patch installation per the Required Customer Actions outlined in this notification.

Verification Form		
Company Name		
Product/Device Name	**QTY**	**Serial Number(s)**
Check all that applies ☐ NextSeq 550Dx ☐ MiSeqDx ☐ Stand-alone instances of the off-instrument LRM for RUO mode on the Dx instruments.		
Your Information		
Print Name:		
Print title of person completing form:		
Customer Responses		
I confirm receipt of FSN2022 - 1230 and that I read and understood its content	Yes ☐ No ☐	

Technical Support:
techsupport@illumina.com

Customer Care:
customercare@illumina.com

I acknowledge that LRM is installed on instrument(s) that are checked above.	Yes ☐ No ☐
The information has been brought to the attention of all relevant users.	Yes ☐ No ☐
I confirm that the software patch is installed on all instruments identified above.	Yes ☐ No ☐
Distributor/Importer Responses	**Not applicable ☐**
I have identified customers that received or may have received the product.	Yes ☐ No ☐
I have informed the identified customers of this recall.	Date (DD-MON-YYYY)

I understand that upon downloading the software patch, it needs to be installed separately on each mode (Dx mode and RUO mode, respectively) of each and every affected instrument identified in this Verification Form and/or any stand-alone instances of the off-instrument LRM for RUO mode on the Dx instruments.

Signature of Person Completing Form

Date

Technical Support:
techsupport@illumina.com

Customer Care:
customercare@illumina.com