Recall

illumina

Wednesday, May 8, 2024

Quality Notification
Urgent Medical Device Recall
Urgent Field Safety Notice

Dear Customer,

Illumina is contacting you regarding a cybersecurity vulnerability identified in the communication protocol between the customer-provided network storage, servers and/or computers and the products specified in Table 1 below. This notice outlines the issue summary, Illumina actions, and required customer actions.

Table 1: Affected Product(s)

Product Affected	Catalog Number	Unique Device Identifier - Device Identifier Number
MiSeq™ Dx Instrument	DX-410-1001 / 15036706	00816270020002
NextSeq™ 550Dx Instrument	20005715	00816270020125
NovaSeq™ 6000Dx Instrument	20068232	00816270020637
Illumina DRAGEN™ Server for NextSeq™ 550Dx	20086130	N/A
Illumina DRAGEN™ Server v4	20051343	N/A
VeriSeq™ Onsite Server v2	20047000	N/A

Issue Summary

While conducting routine cybersecurity analysis, Illumina's Product Security Team identified an uncontrolled product security risk associated with the communication protocol between Illumina's products identified in Table 1 and customer-provided network storage, servers and/or computers. Illumina determined that, if secure protocols are not used, an unauthorized actor who has already gained privileged access to the customer network could intercept and exploit these communications.

If an unauthorized actor were to exploit this vulnerability, they potentially could intercept and

modify files, leading to delivery of incorrect results, delayed results, no results, or corrupted files to customer-provided network entity, and/or exposure of patient data in the transmitted files.

At this time, Illumina has not received any reports and has no evidence indicating that this vulnerability has been exploited.

Illumina Actions

Illumina is providing Cybersecurity Guidance that includes recommendations on how customers can secure their internal network's communication with Illumina's product.

Failure to follow these instructions or implement network security best practices to protect your systems could leave your organization exposed to the risks described above.

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

Required Customer Actions

For all the affected products, please take the following actions to implement the mitigations:

1. Download & read this Cybersecurity Guidance document. The full hyperlink is below.
   https://support.illumina.com/support-content/cyberguidance.html
2. For Each Product Connected to the Customer Network: work with your internal IT department to determine which secure protocol works best in your environment and to implement the appropriate configuration change.

Note: *a change to the network protocol affects both Dx and RUO modes simultaneously therefore there is no need to boot into each mode separately to take the necessary action.*

Complete and return the Verification Form after carrying out all the steps in the instructions provided on your specific product(s) identified as affected in Table 1.

NOTE: If you suspect your product may have been compromised by an unauthorized actor, please immediately unplug the network cable and contact techsupport@illumina.com.

If you experience an adverse event due to this vulnerability with the use of any 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 security issues very seriously. We are committed to supporting you in addressing this vulnerability. For any other questions or assistance, please contact techsupport@illumina.com. You may also be contacted by an external vendor on behalf of Illumina to ensure that you have the support you need.

Why You're Receiving This Notification

You are receiving this notification because our records indicate that you are the appropriate contact for your organization for product changes, product obsolescence, and quality issues.
Please be aware that these notifications contain essential information about our products and are not marketing communications. As such, you may receive these notifications despite having opted-out of receiving marketing communications from Illumina. If you are not the appropriate individual in your organization to receive these notifications, you may unsubscribe from these notifications by submitting this form. For more information, please see our Privacy Policy.

Technical Support:
techsupport@illumina.com

Customer Care:
customercare@illumina.com

Verification Form

Dear Customer,

Illumina sent you an Urgent Medical Device Recall Notice FSN2024-1562 regarding an issue affecting the NextSeq 550Dx, MiSeqDx, NovaSeq 6000Dx instruments, the Illumina DRAGEN Server for NextSeq 550Dx, the Illumina DRAGEN Server v4, and the VeriSeq Onsite Server v2.

Please complete the form below to confirm that you have received the notice and completed the Required Customer Actions outlined in this notification. Once completed, please email the form to techsupport@illumina.com.

Alternatively, you may e-mail Illumina Technical Support to provide the information requested below.

Verification Form	
Company Name	
Information of Person Completing Form	
Name:	
Title:	
Date (DD-MMM-YYYY):	
Customer Responses	
I confirm receipt of FSN2024-1562 and that I read and understood its content.	☐Yes ☐ No
The information has been brought to the attention of all relevant users.	☐Yes ☐ No
I confirm that the Cybersecurity Guidance Document has been downloaded and read.	☐Yes ☐ No

Distributor/Importer Responses	☐ Not applicable
I have identified customers that received or may have received the affected product.	☐ Yes ☐ No
I have informed the identified customers of this recall.	☐ Yes ☐ No Date (DD-MMM-YYYY):

Technical Support:
techsupport@illumina.com

Customer Care:
customercare@illumina.com