Recall

illumina

Tuesday, September 17, 2024

Quality Notification
Urgent Medical Device Recall
Urgent Field Safety Notice

Dear Customer,

Illumina is contacting you regarding a security vulnerability identified in the Baseboard Management Controller (BMC) in the DRAGEN™ Server for the NovaSeq™ 6000Dx instruments and Illumina DRAGEN Server for NextSeq™ 550Dx instruments. Affected servers are specified in Table 1 below. This notice outlines the issue summary, Illumina actions, and required customer actions. Please note, this security vulnerability is limited to these Illumina DRAGEN Servers. Other versions of DRAGEN Servers are not impacted.

Table 1: Affected Products

Product Affected	Catalog Number	Unique Device Identifier - Device Identifier Number
NovaSeq 6000Dx Instrument including DRAGEN Server	20068232	00816270020637
Illumina DRAGEN Server for NextSeq 550Dx	20086130	N/A

Issue Summary

The Illumina Product Security Team has identified an uncontrolled product security risk associated with the Baseboard Management Controller (BMC) used in the DRAGEN Servers listed above. The security vulnerability is due to an insecure user account in the BMC module that is enabled by default.

Illumina has determined that if an unauthorized actor were to exploit this vulnerability the actor could access the BMC remote console without providing a password (authentication bypass). Exploitation of this vulnerability could lead to unauthorized system access, manipulation of hardware settings, remote code execution, remote control, data breaches and denial of service.

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 customers with instructions on how to secure their server which will remediate and protect their systems against exploitation of this vulnerability.

Failure to follow these instructions could leave your system 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 affected DRAGEN Servers listed in Table 1 above, please take the following actions to remediate this critical security vulnerability:

- Download and follow the Customer Instructions from this webpage. The full hyperlink is below: https://support.illumina.com/support-content/bmc.html

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

NOTE: If you suspect your server 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 security vulnerability with the use of any of the affected servers, 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.

Sincerely,

Gary Workman

Electronically signed by:
Gary Workman
Reason: Approver
Date: Sep 6, 2024 10:17 EDT

Gary Workman
Vice President of Global Quality

Karen Gutekunst

Electronically signed by:
Karen Gutekunst
Reason: Approver
Date: Sep 4, 2024 07:57 PDT

Karen Gutekunst
Vice President of Regulatory Affairs

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 FSN2024-1635 regarding an issue affecting the DRAGEN Servers for the NovaSeq 6000Dx and NextSeq 550Dx instruments.

Please complete the form below to confirm that you have received the notice and completed the Required Customer Actions outlined in the 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):	
Server Name	**Serial Number(s)**
DRAGEN Server for NovaSeq 6000Dx	
Illumina DRAGEN Server for NextSeq 550Dx	
Customer Responses	
I confirm receipt of FSN2024-1635 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 remediation steps listed in the Required Customer Actions section have been implemented on each and every affected server identified in this verification form.	☐Yes ☐ No

Technical Support:
techsupport@illumina.com

Customer Care:
customercare@illumina.com

Distributor/Importer Responses	☐ Not applicable
I have identified customers that received or may have received the affected servers.	☐ 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