Our role in a connected healthcare system

Illumina response to recent LRM cybersecurity vulnerability

Background

At Illumina, we are proud to support a connected healthcare system that accelerates innovation and delivers cutting-edge therapies to patients by sharing genomic and health data at scale.

One risk facing participants in the emerging space of digital genomic science is exposure to cybersecurity vulnerabilities.

As Illumina encourages and contributes to a connected healthcare ecosystem, we know that we must address cybersecurity vulnerabilities as we work to mitigate cyber risks and prevent data loss.

This post addresses a cybersecurity vulnerability affecting Illumina Local Run Manager (LRM) desktop instrument software. This vulnerability was communicated to customers beginning May 3, 2022.

As we work with our customers to continuously improve security, this post also highlights certain security best practices that we recommend for customers.

Summary of recent issue

Illumina has validated and provided a short-term patch for a remote code execution vulnerability affecting Local Run Manager, communicated to customers starting on May 3, 2022. Illumina has notified regulatory bodies of this issue globally.

Local Run Manager is part of the default configuration of the following instruments: NextSeq™ 550Dx, MiSeq™Dx, NextSeq 500/550, MiSeq, iSeq™, and MiniSeq™ systems. It is also offered as an off-instrument software that can be installed on customer-provided hardware.

This vulnerability is an unauthenticated Remote Command Execution (RCE), meaning an unauthorized user who can bypass security controls could potentially exploit the system and act at an administrator level, including taking actions that could impact settings, configurations, software, or data on the instrument or the customer's network.

Mitigation and remediation

The Illumina software team has developed a software patch to protect against remote exploitation of this vulnerability. In addition to this patch, we are working to provide a permanent software fix for current and future instruments and will notify customers directly when it is available.

Additional security recommendations

Secure deployment of research use only (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. We also strongly advise using firewalls and other network policies to restrict inbound and outbound access.

Looking ahead

We are supporting our customers to install the software patch for this issue immediately and to promptly implement the long-term solution when available. Illumina will continue to assess and enhance our systems to maintain a strong cybersecurity posture to support continuous innovation in healthcare.

It is essential that all participants in the connected healthcare system are proactive and vigilant about cybersecurity, including adopting best practices and implementing short- and long-term solutions to identified vulnerabilities.

We believe that aggregated and connected genomic data greatly benefits healthcare innovation and impact, from basic research to vaccine development. We look forward to continuing to work in close partnership with our customers to realize the benefits of a connected healthcare ecosystem and to improve human health by unlocking the power of the genome.

illumina®

1.800.809.4566 toll-free (US) | +1.858.202.4566 tel
techsupport@illumina.com | www.illumina.com

M-GL-00810 v1.0