La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) y la Administración de Alimentos y Medicamentos (FDA), emitieron un aviso sobre las vulnerabilidades de seguridad críticas en el software de secuenciación de próxima generación (NGS) de Illumina.

Tres de las vulnerabilidades tienen una calificación de 10 sobre 10 en gravedad en el Sistema de Puntuación de Vulnerabilidad Común (CVSS), y otras dos tienen calificaciones de gravedad de 9.1 y 7.4.

Los problemas afectan al software en los dispositivos médicos que se utilizan para *«uso de diagnóstico clínico en la secuenciación del ADN de una persona o pruebas para diversas afecciones genéticas, o solo para uso en investigación»*, según la FDA.

> *«La explotación exitosa de estas vulnerabilidades puede permitir que un actor malicioso no autenticado tome el control del producto afectado remotamente y realice cualquier acción a nivel del sistema operativo»*, dijo CISA en una alerta.

> *«Un atacante podría afectar la configuración, el software o los datos del producto afectado e interactuar a través del producto afectado con la red conectada».*

Los dispositivos afectados e instrumentos afectados incluyen: NextSeq 550Dx, MiSeq Dx, NextSeq 500, NextSeq 550, MiSeq, iSeq 100 y MiniSeq con las versiones 1.3 a 3.1 del software Local Run Manager (LRM).

Las vulnerabilidades son las siguientes:

- CVE-2022-1517 (Puntaje CVSS: 10): Una vulnerabilidad de ejecución remota de código a nivel del sistema operativo que podría permitir que un atacante altere la configuración y acceda a datos confidenciales o API.

- CVE-2022-1518 (puntaje CVSS: 10): Una vulnerabilidad transversal de directorio que podría permitir que un atacante cargue archivos maliciosos en ubicaciones arbitrarias.
- CVE-2022-1519 (puntaje CVSS: 10): Un problema con la carga sin restricciones de cualquier tipo de archivo, lo que permite a un atacante lograr la ejecución de código arbitrario.
- CVE-2022-1521 (puntaje CVSS: 9.1): Falta de autenticación en LRM de forma predeterminada, lo que permite a un atacante inyectar, modificar o acceder a datos confidenciales.
- CVE-2022-1524 (puntaje CVSS: 7.4): Falta de cifrado TLS para las versiones 2.4 y anteriores de LRM que podría ser objeto de abuso por parte de un atacante para organizar un ataque de intermediario (MitM) y acceder a las credenciales.

Además de permitir el control remoto de los instrumentos, las vulnerabilidades podrían usarse como armas para comprometer las pruebas clínicas de los pacientes, lo que resultaría en resultados incorrectos o alterados durante el diagnóstico.

Aunque no hay evidencia de que las fallas se estén explotando en la naturaleza, se recomienda que los clientes apliquen el parche de software lanzado por Illumina el mes pasado para mitigar cualquier riesgo potencial.