НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220603.2 | 3 июня 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Illumina Local Run Manager

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	In Vitro Diagnostic NextSeq 550Dx: All versions In Vitro Diagnostic MiSeq Dx: All versions NextSeq 500 Instrument: All versions NextSeq 550 Instrument: All versions MiSeq Instrument: All versions iSeq 100 Instrument: All versions MiniSeq Instrument: All versions Local Run Manager (LRM): 1.3 - 3.1
Дата выявления	03 июня 2022 г.
Дата обновления	03 июня 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS

MITRE: CVE-2022-1517	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с привилегиями root в целевой системе посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена некорректным битом setuid в двоичном файле уязвимого приложения. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-250: Выполнение операций с избыточными привилегиями Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	10.0
MITRE: CVE-2022-1518	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить обход каталогов посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	10.0
MITRE: CVE-2022-1519	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить вредоносный файл и запустить на уязвимом сервере. Уязвимость обусловлена некорректной проверкой файла во время загрузки. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-434: Отсутствие ограничений на загрузку файлов небезопасного типа Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	10.0

MITRE: CVE-2022-1521	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректными ограничениями доступа. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	9.1

Ссылки на источники	http://ics-cert.us-cert.gov/advisories/icsa-22-153-02