Министерство здравоохранения
Российской Федерации
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ
В СФЕРЕ ЗДРАВООХРАНЕНИЯ
(РОСЗДРАВНАДЗОР)

Славянская пл. 4, стр. 1, Москва, 109012
Телефон: (499) 578 06 70; (499) 578 02 20
www.roszdravnadzor.gov.ru

05.09.2022 № 01и-942/22

На № _____ от _____

О безопасности
медицинских изделий

2524147

Субъектам обращения
медицинских изделий

Руководителям
территориальных
органов Росздравнадзора

Медицинским организациям

Органам управления
здравоохранением субъектов
Российской Федерации

Федеральная служба по надзору в сфере здравоохранения в рамках исполнения государственной функции по мониторингу безопасности медицинских изделий, находящихся в обращении на территории Российской Федерации, доводит до сведения субъектов обращения медицинского изделия письмо ООО «Сименс Здравоохранение», уполномоченного представителя производителя медицинского изделия, о новых данных по безопасности при применении медицинского изделия «Аппарат рентгеновский медицинский диагностический AXIOM ARTIS с С-дугой для универсальной и кардиологической ангиографии, модели: MP, FC, FA, BC, BA», производства «Сименс АГ Медикал Солюшенс», Германия, регистрационное удостоверение МЗ РФ № 2002/269 от 07.05.2002 до 07.05.2012.

В случае необходимости получения дополнительной информации обращаться в ООО «Сименс Здравоохранение» по контактным данным: тел.: 8 (495) 737 12 52; адрес: Россия, 115093, Москва, ул. Дубнинская, 96.

Приложение: на 4 л. в 1 экз.

А.В. Самойлова

Приложение к письму Росздравнадзора
от 05.09.2022 № 01и-942/22

SIEMENS Healthineers

Siemens Healthcare GmbH, HC AT IR MK, Siemensstr. 1, 91301 Forchheim

Всем пользователям систем Artis, X-Workplace, Sensis и Arcadis с устаревшим аппаратным или программным обеспечением

ФИО Д-р Филип Стеннер
Отдел HC AT IR MK
Адрес электронной почты philip.stenner@siemens-healthineers.com

Дата 26 мая 2017 г.

Важное уведомление о проблемах безопасности: **AX047/17/S**

Информация о возможной уязвимости в операционной системе Microsoft Windows, установленной на системах Artis, X-Workplace, Sensis и Arcadis.

Уважаемый клиент!

Настоящим письмом информируем Вас о возможной проблеме безопасности, связанной с защищенностью системы, которая может быть опасна для пациентов.

В чем состоит основная проблема и когда она возникает?

Системы Artis, X-Workplace, Sensis и Arcadis работают на базе операционных систем Windows XP и Windows 7. Из-за уязвимости этих операционных системах имеется основание для кратковременной опасности.
Вредоносное программное обеспечение, известное как вирус "WannaCry", использует эту уязвимость для проникновения в незащищенные системы и повреждения данных на этих системах путем шифрования.

Дополнительная техническая информация содержится в пояснении Siemens, доступном в Интернете:
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-023589.pdf

Как это отражается на работе системы и в чем состоит потенциальная опасность?

Это вредоносное программное обеспечение зашифровывает данные на пораженных системах. Шифрование определенных компонентов систем Artis, X-Workplace, Sensis или Arcadis может привести к ситуации, когда необходимо отменить или перезапустить клиническое лечение либо перенести его в функционирующую систему.
Кроме того, могут быть потеряны ранее полученные данные.

Какое действие можно предпринять?

Риск использования любой из подобных уязвимостей зависит от фактической конфигурации и среды развертывания каждого изделия. По заявлению компании Microsoft эта вредоносная программа распространяется в виде вложений или ссылок в электронных письмах, рассылаемых фишинг-мошенниками, либо на вредоносных веб-сайтах (т. н. "уязвимость нулевого дня"), а также посредством зараженной системы, использующей уязвимость в компоненте Windows, который применяется в контексте открытого совместного использования файлов других систем, доступ к которым можно получить в одной сети. Определенные сведения доступны на следующей странице Microsoft:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacryptattacks/

Необходимо отметить, что использование клиента электронной почты или просмотр страниц в Интернете не относятся к использованию большинства типов изделий по назначению.

Рекомендации

В системах, к которым относится данное письмо, и которые перечислены в следующем абзаце, используется устаревшее аппаратное и программное обеспечение.
Для следующих систем нельзя применять исправление Microsoft Patch.

Arcadis:

Arcadis Varic	(шифр: 8080017)
Arcadis Orbic	(шифр: 8081080)
Arcadis Avantic	(шифр: 10048590)
Arcadis Varic Gen2	(шифр: 10143406) до шифра 15000
Arcadis Orbic Gen2	(шифр: 10143407) до шифра 23000
Arcadis Avantic Gen2	(шифр: 10143408) до шифра 33000

syngo X-WP:

X-Leonardo	VA70, VA71, VA72, VB11A/B, VB11M,

Для прослушивания вышеупомянутых устройств используются сетевые порты 139/tcp, 445/tcp или 3389/tcp.
Степень их защищенности от внешнего воздействия зависит от мер безопасности, принятых в сети. Для защиты уязвимого изделия от внешнего воздействия его необходимо изолировать от любых потенциально зараженных систем в соответствующем сегменте сети (например, изделие, используемое в сегменте сети, отделенном с помощью брандмауэра путем блокировки доступа к сетевым портам 139/tcp, 445/tcp и 3389/tcp).

Если вышеуказанные меры невозможно применить, рекомендуется следующее:
При отсутствии рисков для безопасности пациента и его лечения отключите изделие, не пораженное вирусом, от сети и используйте его в автономном режиме.

SIEMENS Healthineers

Для следующих систем рекомендуем обновить устаревшее системное программное обеспечение до современной версии, для которой можно применить исправление Microsoft Patch:

Artis:

AXIOM Artis	VB22N, VB23D/F/G/H/J	→ обновить до VB23P
AXIOM Artis	VB30C/E, VB31E/F, VB35A	→ обновить до VB35E
Artis zee	VC13A/B, VC13D/E, VC14B/D/E/G	→ обновить до VC14J
Artis zee	VC21A	→ обновить до VC21C
Artis One	VA10B, VA10C	→ обновить до VA10D

syngo X-WP:

syngo X-WP	VB13E	→ обновить до VB13F
syngo X-WP	VB14A, VB14B	→ обновить до VB14C
syngo X-WP	VB15B, VB15C	→ обновить до VB15D
syngo X-WP	VB20B, VB20C	→ обновить до VB20D
syngo X-WP	VB21B	→ обновить до VB21C
syngo X-WP	VC10C	→ обновить до VC10D

Sensis:

Sensis	VC03A/B/C/D	→ обновить до VC03G или более поздней версии
Sensis	VC10B/C, VC11A/B/C	→ обновить до VC11D или более поздней версии
Sensis	VC12A	→ обновить до VC12C или более поздней версии
Sensis	VC12K	→ обновить до VC12L или более поздней версии

Кроме того, компания Siemens Healthineers рекомендует следующее:

Обеспечьте выполнение надлежащих процедур резервного копирования и восстановления системы.

Каким образом была выявлена проблема?

Угроза была обнаружена при оповещении о заражении определенного частного, промышленного и медицинского оборудования. Необходимо принимать во внимание возможность существования соответствующей уязвимости систем Artis, X-Workplace, Sensis и Arcadis.

SIEMENS Healthineers

В чем заключаются риски для пациентов, ранее прошедших обследование или лечение с использованием этой системы?

В этом случае нет необходимости проводить повторное обследование этих пациентов. Этот потенциальный дефект не влияет на лечение пациентов.

Благодарим Вас за сотрудничество в связи с данным уведомлением пользователей о проблемах безопасности и просим в кратчайшие сроки уведомить сотрудников Вашего учреждения об этой проблеме и предоставить соответствующие инструкции. Направьте эту информацию в другие учреждения, где эта проблема может иметь место.

Если Вы больше не являетесь владельцем устройства по причине его продажи, перенаправьте это уведомление новому владельцу. Мы также просим Вас предоставить нам контактные данные нового владельца, если это возможно.

С уважением,

Siemens Healthcare GmbH
AT Business Area

Д-р Хайнрих Колем
Президент отдела передовых методов терапии

Вольфганг Хофманн
Специалист по безопасности медицинского оборудования