МИНИСТЕРСТВО
ОБРАЗОВАНИЯ
САРАТОВСКОЙ ОБЛАСТИ

ул. Соляная, 32, г. Саратов, 410002
Тел.: (845-2) 49-21-12; факс (845-2) 28-67-49
minobr@minobr.saratov.gov.ru

06.03.2023 № 01-27/1904

на № _____

Руководителям государственных учреждений, функции и полномочия учредителя в отношении которых осуществляет министерство образования Саратовской области (по списку)

В соответствии с письмом Управления делами Правительства Саратовской области от 27 февраля 2023 года № 01-26/292, направляем рекомендации ФСТЭК России о дополнительных мерах по повышению защищенности информационной инфраструктуры для организации выполнения в части, касающейся при наличии в эксплуатации перечисленных видов программного обеспечения.

Приложение: на 4 л. в 1 экз.

Первый заместитель министра **Е.В. Нерозя**

Гитинова Патимат Магомедовна
8 (8452) 49-21-16

Приложение к письму
министерства образования области
от «06» 03 2023г. No 01-17/1904

Дополнительные меры по повышению защищенности информационной инфраструктуры

С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей программного обеспечения необходимо организовать проверку эксплуатируемого программного обеспечения и устранение следующих уязвимостей:

1)Уязвимость программной платформы Cisco IOx (BDU:2023~00549, уровень опасности по CVSS 3.0 -высокий), связанная с недостаточной проверкой входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнять произвольные команды в операционной системе с привилегиями root-пользователя.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года(fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty).

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

отключить функцию Cisco IOx путём ввода команды:

no iox;

выполнить проверку программного средства на подверженность уязвимости осуществляется путём ввода следующей команды:

show iox.

Пример вывода для неуязвимого программно-аппаратного средства (оборудование не подвержено уязвимости, если оно поддерживает собственный Docker и включено Dockerd):

IOx Infrastructure Summary:

IOx service (CAF):Running
IOx service (HA): Running
IOx service (IOxman) : Running
IOx service (Sec storage) : Running
Libvirtd 5.5.0: Running
Dockerd v19.03.13-ce: Running
Sync Status: Disabled

2) Уязвимость гипервизора VMware Workstation (BDU:2023-00571, уровень опасности по CVSS3.0 высокий),

связаннаясошибкамиразграничениядоступа. Эксплуатация уязвимости может позволить нарушителю удалить произвольные файлы в корневой операционной системе.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей корневой операционной системы;

осуществить минимизацию пользовательских привилегий.

3) Уязвимость компонента Upload программного средства для работы с веб-приложениями Oracle Web Applications Desktop Integrator (BDU:2023-00572, уровень опасности по CVSS 3.0 критический), связанная с ошибками при обработке входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить полный контроль над приложением.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

использовать средства межсетевого экранирования уровня веб-приложений для ограничения возможности удаленного доступа.

4) Уязвимость в функции dsi_writeinit реализации протокола Apple Filing Protocol Netatalk (BDU:2023-00621, уровень опасности по CVSS 3.0 критический), связанная с возможностью переполнения буфера на основе кучи. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код в контексте root-пользователя.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

применять системы обнаружения и предотвращения вторжений;

ограничить удаленный доступ к уязвимой корневой операционной системе путем применения средств межсетевого экранирования.

5) Уязвимость домена pesign подсистемы инициализации и управления службами systemd (BDU:2023-00640, уровень опасности по CVSS 3.0 высокий), связанная с возможностью обхода пути. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей;

осуществить принудительную смену паролей пользователей;

ограничить доступ к командной строке для недоверенных пользователей;

использовать антивирусные средства защиты;

производить мониторинг действий пользователей.

6) Уязвимость декларативного инструмента непрерывной доставки GitOps для Kubernetes ArgoCD (BDU:2023~00641, уровень опасности по CVSS 3.0 высокий), связанная с недостатками процедуры авторизации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

отключить сегментирование в контроллере приложений;

отключить функцию «apps-in-any-namespace»;

использовать запуск только одной реплики контроллера;

ограничить пространства имен приложений AppProjects только существующими и ранее настроенными.

7) Уязвимость VPN-сервера Cisco AnyConnect сетевых устройств Cisco Meraki MX и Cisco Meraki Z3 Teleworker Gateway {BDU:2023-00690, уровень опасности по CVSS 3.0 высокий), связанная с ошибками при обработке функцией отсутствующего параметра. Эксплуатация уязвимости может

позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

использовать средства межсетевого экранирования;

обеспечить применение систем обнаружения и предотвращения вторжений.

8) Уязвимость компонента Windows Graphics операционных систем Windows (BDU:2023-00755, уровень опасности по CVSS 3.0 высокий), связанная с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

использовать средства антивирусной защиты для ограничения возможности эксплуатации уязвимости;

использовать замкнутую программную среду;

осуществить минимизацию пользовательских привилегий;

производить мониторинг действий пользователей;

отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей.