# Министерство
# цифрового развития Республики Мордовия

**Мордовия Республикань цифровой развитиянь Министерствась**

**Мордовия Республикань цифровой развитиянь Министерствась**

*Коммунистическая ул., д. 33, корп. 3, г. С а р а н с к, 430005. Тел. / факс 8 (834-2) 39-14-01 / 39-14-02*
*e-mail: mininformsvyaz@e-mordovia.ru*
ОКПО 916833714, ОГРН 1121326001554, ИНН 1326221952, КПП 132601001

18.03.2024 №4-494

На №_____от_____

Руководителям органов государственной власти Республики Мордовия

Руководителям органов местного самоуправления в Республике Мордовия

Руководителям организаций

(по списку)

В целях повышения защищённости информационной инфраструктуры Республики Мордовия, а также предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей программного обеспечения, направляем прилагаемые рекомендации Управления ФСТЭК России по Приволжскому федеральному округу для принятия мер по их устранению (при наличии).

В соответствии с пунктом 10 Регламента по выявлению, анализу, реагированию и устранению критичных уязвимостей в информационных системах, эксплуатируемых в органе (организации), одобренном на заседании Совета по защите информации при Правительстве Республики Мордовия 22 декабря 2023 года (РК № 1484 – РМ/6 от 7 декабря 2023 года) просим проинформировать Министерство цифрового развития Республики Мордовия о фактически принятых мерах до 5 апреля 2024 года.

И.о. Министра цифрового развития Республики Мордовия — Р.Р. Курмакаев

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 009483FCB8DC636A2235A05821267A9786
Владелец **Курмакаев Роман Равилевич**
Действителен с 09.11.2023 по 01.02.2025

А.Н. Петухов

Исп. Петухов Анатолий Николаевич ☎ +7 (8342) 39-14-24, petukhovan@e-mordovia

39-14-24

Приложение

# РЕКОМЕНДАЦИИ
## Управления ФСТЭК России по Приволжскому федеральному округу по повышению защищенности информационной инфраструктуры органов власти Республики Мордовия

1. Уязвимость средства обеспечения безопасности конечных точек Cisco Secure Client (ранее Cisco AnyConnect Secure Mobility Client) (BDU:2024-01868, уровень опасности по CVSS 3.0 высокий), связанная с непринятием мер по нейтрализации CRLF-последовательностей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в браузере при условии перехода пользователем по вредоносной ссылке.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2).

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

– отключить функционал внешнего браузера SAML;

– использовать антивирусное программное обеспечение при переходе по ссылкам, полученным из недоверенных источников;

– использовать средства межсетевого экранирования уровня веб-приложений для предотвращения возможности эксплуатации уязвимости.

2. Уязвимость значения pga4_session файла cookie-сеанса инструмента управления базами данных pgAdmin 4 (BDU:2024-01869, уровень опасности по CVSS 3.0 высокий), связанная с некорректной сериализацией. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2).

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

использовать pgAdmin в режиме рабочего стола для предотвращения возможности эксплуатации уязвимости;

– отключить (удалить) неиспользуемые учётные записи пользователей;

– произвести минимизацию пользовательских привилегий; ограничить доступ из внешних сетей (Интернет);

– использовать виртуальные частные сети для организации удаленного доступа.

3. Уязвимость операционных систем QTS, QuTS Hero, QuTScloud и myQNAPcloud (BDU:2024-01870, уровень опасности по CVSS 3.0 критический), связанная с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить полный доступ к устройству, управляемому уязвимой операционной системой.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2).

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

– ограничить доступ к устройствам Qnap из общедоступных сетей; использовать средства межсетевого экранирования уровня веб-приложений для ограничения возможности удалённого доступа;

– использовать виртуальные частные сети для организации удаленного доступа.

4. Уязвимость программных средств для резервного копирования и восстановления данных Veritas NetBackup и Veritas NetBackup Appliance (BDU:2024-01877, уровень опасности по CVSS 3.0 критический), связанная с неверным ограничением имени пути к каталогу с ограниченным доступом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2).

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

– ограничить доступ к программному обеспечению из общедоступных сетей;

– использовать средства межсетевого экранирования уровня веб-приложений для ограничения возможности удалённого доступа;

– использовать системы обнаружения и предотвращения вторжений для отслеживания попыток эксплуатации уязвимости.

5. Уязвимость функции getblockschedule() анализа JSON встроенного программного обеспечения маршрутизаторов NETGEAR RAX28, RAX29, RAX30 (BDU:2024-01918, уровень опасности по CVSS 3.0 высокий), связанная с возможностью переполнения буфера на основе стека. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код путём отправки специально сформированного HTTP-запроса.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2).

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

– использовать средства межсетевого экранирования уровня веб-приложений для ограничения возможности удалённого доступа;

– отключить (удалить) неиспользуемые учётные записи пользователей; ограничить доступ к устройству из внешних сетей;

– использовать виртуальные частные сети для организации удаленного доступа.