



**МИНИСТЕРСТВО
ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ АСТРАХАНСКОЙ ОБЛАСТИ**

Адмиралтейская ул., стр. 53А,

г.о. город Астрахань, 414040

Е-mail: mingos@astrobl.ru

18.08.2026 № 111-01-14/3544

На № _____ от _____

Руководителям
исполнительных органов
Астраханской области
(по списку)

Главам
муниципальных районов,
муниципальных округов,
городских округов
Астраханской области
(по списку)

Уважаемые руководители!

В соответствии с прилагаемым письмом Управления ФСТЭК России по Южному и Северо-Кавказскому федеральным округам от 14.08.2026 № 4/9/741-эп (далее – письмо) о предотвращении реализации угроз безопасности информации министерство государственного управления, информационных технологий и связи Астраханской области (далее – министерство) обращает ваше внимание на необходимость устранения следующих уязвимостей программного обеспечения.

1. Уязвимость механизма автоматического обновления программного комплекса защиты информации ViPNet Client 4 (BDU:2026-09885, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками обработки относительных путей. Эксплуатация уязвимости может позволить злоумышленнику, действующему из смежной доверенной сети, нарушить целостность среды функционирования, повысить привилегии в системе атакуемого узла и выполнить на нем произвольный код путем использования специально сформированного пакета обновления, отправляемого от имени скомпрометированного доверенного узла с ролью ЦУС (Центр управления сетью).

2. Уязвимость механизма управления теневыми таблицами страниц (Shadow MMU) подсистемы виртуализации Kernel-based Virtual Machine (KVM) ядра операционной системы Linux (BDU:2026-11388, уровень опасности по CVSS 3.1 – высокий), связанная с разыменованием указателя с истекшим сроком действия. Эксплуатация уязвимости может позволить злоумышленнику повысить свои привилегии, выполнить произвольный код или вызвать отказ в обслуживании.

3. Уязвимость функции `sctp_process_asconf_param()` модуля `net/sctp/sm_make_chunk.c` ядра операционных систем Linux (BDU:2026-11391, уровень опасности по CVSS 3.1 – критический), связанная с разыменованием указателя с истекшим сроком действия. Эксплуатация уязвимости может позволить злоумышленнику, действующему удаленно, повысить свои привилегии до уровня `root`.

4. Уязвимость драйвера вспомогательной функции `afd.sys` для WinSock операционных систем Windows (BDU:2026-11398, уровень опасности по CVSS 3.1 – высокий), связанная с возможностью использования памяти после освобождения. Эксплуатация уязвимости может позволить злоумышленнику повысить свои привилегии.

5. Уязвимость компонента Skia веб-браузеров Google Chrome и Microsoft Edge (BDU:2026-11032, уровень опасности по CVSS 3.1 – высокий), связанная с ошибками обработки HTTP-запросов. Эксплуатация уязвимости может позволить злоумышленнику, действующему удаленно, вызвать отказ в обслуживании с помощью специально созданной HTML-страницы.

6. Уязвимость функционала импорта/экспорта данных (Import/Export Data) инструмента управления базами данных pgAdmin 4 (BDU:2026-11412, уровень опасности по CVSS 3.1 – критический), связанная с непринятием мер по нейтрализации специальных элементов. Эксплуатация уязвимости может позволить злоумышленнику, действующему удаленно, внедрить произвольные команды операционной системы на сервере.

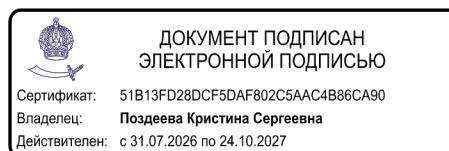
В целях предотвращения возможности эксплуатации указанных уязвимостей программного обеспечения рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28.10.2022, а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30.06.2025.

В случае невозможности установки обновления программного обеспечения рекомендуется принять компенсирующие меры, указанные в письме Управления ФСТЭК России, а также на соответствующих страницах Банка данных угроз безопасности информации (<https://bdu.fstec.ru/vul>).

С учетом вышеизложенного просим проинформировать подведомственные учреждения, а также предоставить в адрес министерства в срок до 31.08.2026 обобщенные сведения о выполненных мероприятиях.

Приложение: на 8 л. в 1 экз.

Заместитель министра



К.С. Поздеева

Кулешова Алена Вадимовна
(8512) 66-99-88 (доб. 1142)