Бюллетень информационной безопасности от 04.09.2025

I. Сведения об уязвимостях.

Обращаем внимание на зафиксированные специалистами ФСТЭК России уязвимости, отнесенные к категории «наиболее опасные уязвимости».

1. Уязвимость браузеров Mozilla Firefox, Firefox ESR и почтового клиента Thunderbird (BDU:2025-09461, уровень опасности по CVSS 3.0 – высокий), связанная с раскрытием информации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, оказать воздействие на конфиденциальность и целостность защищаемой информации.

2. Уязвимость функции reqsk_queue_unlink() модуля net/ipv4/inet_connection_sock.c ядра операционной системы Linux (BDU:2025-03473, уровень опасности по CVSS 3.0 – высокий), связанная с повторным использованием ранее освобожденной памяти. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

3. Уязвимость драйвера общей файловой системы журналов операционных систем Windows (BDU:2024-06424, уровень опасности по CVSS 3.0 – высокий), связанная с недостаточной проверкой входных данных. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

4. Уязвимость функции bnxt_re_ib_get_hw_stats() в модуле drivers/infiniband/hw/bnxt_re/hw_counters.c ядра операционной системы Linux (BDU:2025-00169, уровень опасности по CVSS 3.0 – высокий), связанная с чтением памяти за пределами выделенного буфера. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

В целях предотвращения возможности эксплуатации указанных в пунктах 1-4 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28.10.2022 (далее – «Методика тестирования»), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30.06.2025 (далее – «Методика оценки») (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty).

5. Уязвимость службы wuauserv центра обновлений операционной системы Windows (BDU:2025-09690, уровень опасности по CVSS 3.0 – высокий), связанная с некорректным определением символических ссылок в ходе осуществления доступа к файлу. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии до уровня system путем выполнения операций удаление/перемещение/переименование директорий.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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

использовать системы обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимости;

минимизировать пользовательские привилегии;

отключить (удалить) неиспользуемые учетные записи пользователей.

6. Уязвимость почтового сервера Microsoft Exchange Server (BDU:2025-09477, уровень опасности по CVSS 3.0 – высокий), связанная с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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

использовать средства межсетевого экранирования для ограничения возможности удаленного доступа к почтовому серверу;

произвести сегментирование сети с целью ограничения доступа к почтовому серверу из других подсетей;

использовать системы обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимости;

минимизировать пользовательские привилегии;

отключить (удалить) неиспользуемые учетные записи пользователей;

использовать виртуальные частные сети для организации удаленного доступа.

7. Уязвимость реализации протокола Kerberos операционных систем Windows (BDU:2025-08180, уровень опасности по CVSS 3.0 – высокий), связанная с ошибками механизма обработки относительного пути к каталогу. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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

использовать средства межсетевого экранирования для ограничения удаленного доступа к уязвимому программному обеспечению;

ограничить доступ к уязвимому программному обеспечению, используя схему доступа по «белым спискам»;

использовать системы обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимостей;

ограничить доступ из внешних сетей.

8. Уязвимость функции unix_stream_read_generic() модуля net/unix/af_unix.c ядра операционных систем Linux (BDU:2025-09670, уровень опасности по CVSS 3.0 – высокий), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии, обойти существующие механизмы безопасности и выполнить произвольный код.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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

использовать SIEM-системы для отслеживания попыток эксплуатации уязвимости;

использовать системы обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимости.

9. Уязвимость файлового архиватора WinRAR (BDU:2025-09597, уровень опасности по CVSS 3.0 – высокий), связанная с неверным ограничением имени пути к каталогу с ограниченным доступом. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код при извлечении специально сформированного файла.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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

использовать антивирусное программное обеспечение для проверки файлов, полученных из недоверенных источников;

использовать SIEM-системы для отслеживания попыток эксплуатации уязвимости;

использовать замкнутую программную среду для работы с файлами, полученными из недоверенных источников.

10. Уязвимость проводника Windows (Windows File Explorer) операционных систем Windows (BDU:2025-09832, уровень опасности по CVSS 3.1 – высокий), связанная с недостаточной защитой служебных данных при обработке NTLM-хешей. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти ограничения безопасности и получить несанкционированный доступ к защищаемой информации путем проведения атаки Zero-click.

11. Уязвимость библиотеки ANGLE браузера Google Chrome (BDU:2025-08785, уровень опасности по CVSS 3.1 – высокий), связанная с недостаточной проверкой входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти существующие ограничения безопасности с помощью специально созданной HTML-страницы.

12. Уязвимость страницы блокировки межсетевого экрана UserGate Next-Generation Firewall (NGFW) (BDU:2025-08181, уровень опасности по CVSS 3.1 – средний), связанная с недостаточной проверкой входных данных. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код при переходе по специально сформированной ссылке.

В целях предотвращения возможности эксплуатации указанных в пунктах 10-12 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

13. Уязвимость реализации протокола SSH из набора библиотек Erlang/OTP (BDU:2025-04706, уровень опасности по CVSS 3.1 – критический), связанная с отсутствием проверки подлинности для критически важной функции. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированных SSH-пакетов.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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

временно отключить SSH-компонент Erlang/OTP или ограничить доступ к порту 22;

использовать средства межсетевого экранирования для ограничения возможности удаленного доступа к уязвимому программному обеспечению;

ограничить доступ к уязвимому программному обеспечению, используя схему доступа по «белым спискам»;

использовать виртуальные частные сети для организации удаленного доступа.

Для осуществления проверки подверженности информационной системы указанной уязвимости рекомендуется выполнить следующие действия с использованием терминала (командной строки):

произвести поиск подозрительных процессов командой:

ps aux | grep -E «(yaso|hello_cve|top1miku)»;

произвести проверку сетевых соединений командой:

netstat -an | grep :22;

произвести анализ журналов службы SSH командой:

journalctl -u ssh | grep -i erlang.

14. Уязвимость драйвера Windows Common Log File System (CLFS) операционных систем Windows (BDU:2025-03926, уровень опасности по CVSS 3.1 – высокий), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии уровня системы. Указанная уязвимость характерна для большинства информационных систем, применяемых в органах государственной власти и субъектах критической информационной инфраструктуры Российской Федерации.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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

использовать SIEM-системы для отслеживания попыток эксплуатации уязвимости;

использовать средства обнаружения и предотвращения вторжений (IDS/IPS) для выявления и реагирования на попытки эксплуатации уязвимости;

минимизировать пользовательские привилегии;

отключить (удалить) неиспользуемые учетные записи пользователей.

15. Уязвимость программной платформы Apache ActiveMQ (BDU:2023-07372, уровень опасности по CVSS 3.1 – критический), связанная с восстановлением в памяти недостоверных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код, путем создания класса по протоколу OpenWire.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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

использовать средства межсетевого экранирования для ограничения возможности удаленного доступа;

ограничить возможность подключения к программной платформе путем внедрения механизма «белых» списков;

использовать виртуальные частные сети для организации удаленного доступа.

16. Уязвимость механизма изоляции контейнеров платформы для разработки и доставки контейнерных приложений Docker Desktop (BDU:2025-10195, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками разграничений контролируемой области системы. Эксплуатация уязвимости может позволить нарушителю получить несанкционированный доступ к API Docker Engine и выполнить произвольные команды путем монтирования специально созданных контейнеров.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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

ограничить возможность монтирования контейнеров из недоверенных источников;

осуществлять верификацию цифровой подписи монтируемых контейнеров;

использовать средства антивирусной защиты для проверки контейнеров, полученных из недоверенных источников;

использовать SIEM-системы для отслеживания событий, связанных с монтированием контейнеров;

использовать средства межсетевого экранирования для ограничения возможности удаленного доступа к уязвимому программному обеспечению;

ограничить доступ к уязвимому программному обеспечению, используя схему доступа по «белым спискам»;

использовать виртуальные частные сети для организации удаленного доступа.