Приложение 2

**Перечень актуальных уязвимостей в программном обеспечении**

Анализ сведений об угрозах безопасности информации в условиях сложившейся геополитической обстановки показывает, что зарубежными хакерскими группировками при реализации компьютерных атак на информационную инфраструктуру Российской Федерации активно эксплуатируются уязвимости программного обеспечения. Для указанных далее уязвимостей имеется информация о наличии средств их эксплуатации, а также об их использовании в реальных атаках на информационную инфраструктуру.

1. Уязвимость проводника Windows (Windows File Explorer) операционных систем Windows версий: Server 2008 и Server 2012 (BDU:2025-09832, уровень опасности по CVSS 3.1 – высокий), связанная с недостаточной защитой служебных данных при обработке NTLM-хэшей. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти ограничения безопасности и получить несанкционированный доступ к защищаемой информации путем проведения атаки Zero-click.

Способ устранения уязвимости: установка обновлений из доверенных источников.

2. Уязвимость библиотеки ANGLE браузера Google Chrome на операционных системах РЕД ОС 7.3, Astra Linux Special 1.7 и 1.8 (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.

Способ устранения уязвимости: установка обновлений из доверенных источников.

3. Уязвимость страницы блокировки межсетевого экрана UserGate Next-Generation Firewall (NGFW) с версией программного обеспечения до 6.1.9.12193R и до 7.3.1.153682R включительно (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.

Способ устранения уязвимости: установка обновлений программного обеспечения до версий 6.1.9.12198R или выше и 7.3.2.183745R или выше.

4. Уязвимость реализации протокола SSH из набора библиотек Erlang/OTP на операционных системах РЕД ОС 7.3, Astra Linux Special 1.7 и 1.8 (BDU:2025-04706, уровень опасности по CVSS 3.1 – критический), связанная с отсутствием проверки подлинности для критически важной функции. Эксплуатация может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированных SSH-пакетов.

Способ устранения уязвимости: установка обновлений из доверенных источников.

Компенсирующие меры: временное отключение SSH-компонента Erlang/OTP или ограничение доступа к порту 22.

5. Уязвимость драйвера Windows Common Log File System (CLFS) операционных систем Windows версий Server 2008 и Server 2012 (BDU:2025-03926, уровень опасности по CVSS 3.1 – высокий), связанная с использованием памяти после ее высвобождения. 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.

Способ устранения уязвимости: установка обновления из доверенных источников.

Компенсирующие меры: минимизация пользовательских привилегий, отключение / удаление неиспользуемых учетных записей пользователей.

6. 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.

Способ устранения уязвимости: установка обновлений из доверенных источников.

Компенсирующие меры: ограничение возможности монтирования контейнеров из недоверенных источников; верификация цифровой подписи монтируемых контейнеров, ограничение доступа к уязвимому программному обеспечению из внешних сетей (Интернет).

7. Уязвимость средства разработки программного обеспечения Microsoft Visual Studio (BDU:2025-10171, уровень опасности по CVSS 3.1 – высокий), связанная с недостаточной проверкой аргументов, передаваемых в команду. Эксплуатация уязвимости может позволить нарушителю выполнить произвольных код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

8. Уязвимость подсистемы Win32 Kernel Subsystem операционных систем Windows версий 10, Server 2008 и Server 2012 (BDU:2025-08480, уровень опасности по CVSS 3.1 – высокий), связанная с ошибкой повторного освобождения памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: установка обновлений из доверенных источников.

9. Уязвимость службы удаленного рабочего стола Remote Desktop Services (RDS) операционных систем Windows версий 10, Server 2019 и Server 2022 (BDU:2024-11193, уровень опасности по CVSS 3.1 – высокий), связанная с использованием небезопасных механизмов обработки аутентификационных данных в памяти операционной системы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

10. Уязвимость сервера приложений Apache Tomcat на операционной системе РЕД ОС 7.3 (BDU: 2025-09900, уровень опасности по CVSS 3.1 – средний), связанная с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, перехватить сеанс и получить доступ к учетной записи пользователя.

Способ устранения уязвимости: установка обновлений из доверенных источников.

11. Уязвимость виртуального графического адаптера VMSVGA программного средства виртуализации Oracle VM VirtualBox (BDU:2025-08589, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками разграничения доступа в результате выхода операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии и выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

12. Уязвимость виртуального контроллера OHCI USB программного средства виртуализации Oracle VM VirtualBox (BDU:2025-08588, уровень опасности по CVSS 3.1 – высокий), связанная с ошибками синхронизации при использовании общего ресурса («Ситуация гонки»). Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии и выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

13. Уязвимость виртуального графического адаптера VMSVGA программного средства виртуализации Oracle VM VirtualBox (BDU:2025-08587, уровень опасности по CVSS 3.1. – высокий), связанная с недостатками разграничения доступа в результате целочисленного переполнения. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии и выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

14. Уязвимость утилиты pg\_dump системы управления базами данных PostgreSQL в операционной системе РЕД ОС 7.3 (BDU:2025-09830, уровень опасности по CVSS 3.1. – высокий), связанная с непринятием мер по защите структуры запроса SQL. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

15. Уязвимость утилиты pg\_dump системы управления базами данных PostreSQL в операционной системе РЕД ОС 7.3 (BDU:2025-09829, уровень опасности по CVSS 3.1 – высокий), связанная с включением функций из недостоверной контролируемой области. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

16. Уязвимость контроллера входящего трафика в кластере Kubernetes ingress-nginx в операционной системе РЕД ОС 7.3 (BDU:2024-06271, уровень опасности по CVSS 3.1. – высокий), связанная с ошибками при обработке аннотаций Ingress-объектов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

Способ устранения уязвимости: установка обновлений из доверенных источников.

17. Уязвимость функции iconv() системной библиотеки glibc в операционной системе Astra Linux Special Edition 1.6 «Смоленск» (BDU:2024-03171, уровень опасности по CVSS 3.1 – высокий), связанная с возможностью записи за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, потенциально выполнить произвольный код путем внедрения специально сформированного PHP-файла.

Способ устранения уязвимости: установка обновлений из доверенных источников.

Компенсирующие меры: минимизация пользовательских привилегий, отключение / удаление неиспользуемых учетных записей пользователей.

18. Уязвимость браузера Yandex Browser версий до 24.7.1.380 (BDU:2024-06704, уровень опасности по CVSS 3.1 – высокий), связанная с использованием ненадежного пути поиска. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код путем загрузки специально сформированного DLL-файла.

Способ устранения уязвимости: обновление программного обеспечения.

19. Уязвимость сервера SMB операционных систем Windows версий 10, 11, Server 2008 – 2025 (BDU:2025-10913, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

Способ устранения уязвимости: установка обновлений из доверенных источников.

Компенсирующие меры: использование механизмов защиты сервера SMBЧ от атак, например, SMB Server Signing и Extended Protection for Authentication (EPA); ограничение доступа из внешних сетей (Интернет).

20. Уязвимость модуля net/vmw\_vsock/virtio\_transport\_common.c ядра Linux операционных систем Astra Linux Special Edition 1.7 и 1.8 (BDU:2024-11660, уровень опасности по CVSS 3.1 – высокий), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

Способ устранения уязвимости: установка обновлений из доверенных источников.

21. Уязвимость реализации протокола NTLM операционных систем Windows версий 10, 11, Server 2008 – 2025 (BDU:2025-11053, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

Способ устранения уязвимости: установка обновлений из доверенных источников.

22. Уязвимость реализации протокола TCP/IP операционных систем Windows версий 10, 11, Server 2008 – 2025 (BDU:2025-04057, уровень опасности по CVSS 3.1. – высокий), связанная с использованием небезопасных механизмов обработки аутентификационных данных в памяти операционной системы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольных код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

23. Уязвимость компонента Windows Kernel операционной системы Windows версий 10, 11, Server 2022 – 2025 (BDU:2025-10035, уровень опасности по CVSS 3.1 – высокий), связанная с возможностью использования памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

24. Уязвимость пакетов программ Microsoft Office версий 2019, LTSC 2021, LTSC 2024 и Microsoft 365 Apps for Enterprise (BDU:2025-10035, уровень опасности по CVSS 3.1 – высокий), связанная с возможностью использования памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код.