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 программного обеспечения TrueConf Server версий: до 5.3.7, до 5.4.6 и до 5.5.1 (BDU:2025-10114, уровень опасности по CVSS 3.1 – высокий), связанная с обходом процедуры аутентификации посредством использования альтернативного пути или канала. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить некоторые запросы к интерфейсу программного приложения (API).

Способ устранения уязвимости: обновление программного обеспечения.

2. Уязвимость программного обеспечения TrueConf Server версий: до 5.3.7, до 5.4.6 и до 5.5.1 (BDU:2025-10114, уровень опасности по CVSS 3.1 – критический), существующая из-за непринятия мер по нейтрализации специальных элементов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: обновление программного обеспечения.

3. Уязвимость сервера обновлений Windows Server Update Service (WSUS) операционных систем Windows версий Server 2012 - 2025 (BDU:2025-12999, уровень опасности по CVSS 3.1 – критический), связанная с недостатками механизма десериализации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: обновление программного обеспечения из доверенных источников.

4. Уязвимость распределенной системы контроля версий Git средства разработки программного обеспечения Microsoft Visual Studio 2019 версий от 16.0 до 16.10 включительно и Microsoft Visual Studio 2022 версий от 17.8 до 17.14 включительно в операционных системах семейства Windows, РЕД ОС 7.3 и Astra

Linux Special Edition 1.8 (BDU:2025-08688, уровень опасности по CVSS 3.1 – высокий), связанная с неправильной авторизацией. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить несанкционированный доступ к защищаемой информации.

Способ устранения уязвимости: обновление программного обеспечения.

5. Уязвимость функции setupLookside() системы управления базами данных SQLite в операционной системе РЕД ОС 7.3 (BDU:2025-13413, уровень опасности по CVSS 3.1 – высокий), связанная с целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

Способ устранения уязвимости: обновление программного обеспечения.

Компенсирующие меры до выхода обновления: минимизировать пользовательский привилегии; отключить (удалить) неиспользуемые учетные записи пользователей.

6. Уязвимость библиотеки для обработки изображений GIMP версий до 3.0.6 (BDU:2025-13626, уровень опасности по CVSS 3.1 – высокий), связанная с записью за границами буфера. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код путем загрузки специально сформированного файла.

Способ устранения уязвимости: обновление программного обеспечения.

7. Уязвимость функции «virtioCoreR3VirtqInfo» команды «VBoxManage debugvm» программного средства виртуализации Oracle VM VirtualBox версий 7.1.12 и 7.2.2 (BDU:2025-10635, уровень опасности по CVSS 3.1 – высокий), связанная с переполнением буфера в стеке. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код и получить несанкционированный доступ к хостовой системе.

Способ устранения уязвимости: обновление программного обеспечения.

Компенсирующие меры: минимизировать пользовательские привилегии; отключить (удалить) неиспользуемые учетные записи пользователей.

8. Уязвимость обработчика LNK-файлов операционных систем Windows (BDU:2025-13635, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками механизма проверки входных данных. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код при открытии специально сформированного файла.

Способ устранения уязвимости: обновление программного обеспечения из доверенных источников.

Компенсирующие меры: ограничение возможности открытия файлов, полученных из недоверенных источников; использование замкнутой программной среды для работы с файлами, полученными из недоверенных источников.

9. Уязвимость ядра операционных систем Windows версий 10, 11, Server 2008 - 2025 (BDU: 2025-11026, уровень опасности по CVSS 3.1 – высокий), связанная с целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: обновление программного обеспечения из доверенных источников.

10. Уязвимость компонента Win32k (Win32k.sys) операционных систем Windows версий 11, Server 2022 - 2025 (BDU:2025-10180, уровень опасности по CVSS 3.1 – высокий), связанная с доступом к ресурсу через несовместимые типы. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: обновление программного обеспечения из доверенных источников.

11. Уязвимость службы Routing and Remote Access Service (RRAS) операционных систем Windows версий Server 2012 - 2025 (BDU:2025-11123, уровень опасности по CVSS 3.1 – высокий), связанная с целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: обновление программного обеспечения из доверенных источников.

12. Уязвимость функции amd_pmc_s2d_init() модуля drivers/platform/x86/amd/pmc.c ядра следующих операционных систем Linux: Astra Linux Special Edition 1.7, 1.8, 4.7, РЕД ОС 7.3 (BDU:2025-03305, уровень опасности по CVSS 3.1 – средний), связанная с ошибками управления ресурсами. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

Способ устранения уязвимости: обновление программного обеспечения.

13. Уязвимость кроссплатформенного гипервизора Xen ядра Linux операционной системы РЕД ОС 7.3 (BDU:2025-12596, уровень опасности по CVSS 3.1 – критический), связанная с ошибками синхронизации при использовании

общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, скомпрометировать уязвимую систему.

Способ устранения уязвимости: обновление программного обеспечения.

14. Уязвимость функции v3d_perfmon_destroy_ioctl() компонента v3d_perfmon.c ядра Linux операционных систем Astra Linux Special Edition 1.7, 1.8, 4.7, РЕД ОС 7.3 (BDU:2025-11953, уровень опасности по CVSS 3.1 – средний), связанная с ошибками разыменования указателя. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

Способ устранения уязвимости: обновление программного обеспечения.

15. Уязвимость компонента fs/nilfs2 ядра Linux операционных систем Astra Linux Special Edition 1.7, 1.8, 4.7 (BDU:2025-07750, уровень опасности по CVSS 3.1 – средний), связанная с ошибками разыменования указателя. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

Способ устранения уязвимости: обновление программного обеспечения.

16. Уязвимость сервера приложений Apache Tomcat в операционной системе РЕД ОС 7.3 (BDU:2025-13742, уровень опасности по CVSS 3.1 – высокий), связанная с обходом относительного пути. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: обновление программного обеспечения.

17. Уязвимость компонента Windows Kernel в операционных системах Windows версий 10, 11, Server 2019 - 2025 (BDU:2025-14039, 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.

Способ устранения уязвимости: установка обновлений из доверенных источников.

18. Уязвимость пакетов программ Microsoft Office версий 2016, 2019, 2021 и 2024 и Microsoft 365 Apps for Enterprise (BDU:2025-10161, уровень опасности по CVSS 3.1 – высокий), связанная с переполнением буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

19. Уязвимость инструмента управления базами данных pgAdmin 4 версий до 9.10 (BDU:2025-14360, уровень опасности по CVSS 3.1 – критический), связанная с неверным управлением генерацией кода. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код при восстановлении данны из PLAIN-файлов.

Способ устранения уязвимости: установка обновлений из доверенных источников.

Компенсирующие меры: использовать средства антивирусной защиты для проверки файлов, полученных из недоверенных источников; использовать замкнутую программную среду для работы с файлами, полученными из недоверенных источников; ограничить доступ из внешних сетей; произвести сегментирование сети для ограничения доступа к уязвимому программному обеспечению.

20. Уязвимость компонента net/sched/sch_hfsc.c ядра Linux операционной систем Astra Linux Special Edition 1.8 (BDU:2025-12349, уровень опасности по CVSS 3.1 – средний), связанная с выполнением цикла с недоступным условием выхода. Эксплуатация уязвимости может позволить нгарушителю получить доступа к конфиденциальным данным, нарушить их целостность, а также вызвать отказ в обслуживании.

Способ устранения уязвимости: обновление программного обеспечения.

21. Уязвимость браузера Mozilla Firefox и почтового клиента Thunderbird до 145 версии (BDU:2025-14088, уровень опасности по CVSS 3.1 – высокий), связанная с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: обновление программного обеспечения.

22. Уязвимость набора инструментов для веб-разработки DevTools браузера Google Chrome в операционных системах РЕД ОС 7.1, Astra linux Special Edition 1.7 и 1.8 (BDU:2025-14028, уровень опасности по CVSS 3.1 – высокий), связанная с неконтролируемым элементом пути поиска. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: обновление программного обеспечения.

23. Уязвимость программного обеспечения мониторинга ИТ-инфраструктуры Checkmk версий до 2.1.0p40, до2.2.0p23, до 2.3.0b1, до 2.4.0b1 для операционных

систем Windows (BDU:2024-02694, уровень опасности по CVSS 3.1 – высокий), связанная с неконтролируемым элементом пути поиска. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: обновление программного обеспечения.

24. Уязвимость компонента Host Process операционной системы Windows версии 11 (BDU:2025-14198, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: установка обновлений из доверенных источников.

25. Уязвимость сервера обновлений Windows Server Update Services (WSUS) операционных систем Windows версий Server 2012 - 2022 (BDU:2023-04209, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: установка обновлений из доверенных источников.

26. Уязвимость компонента Recovery Environment Agent операционных систем Windows версий 10, 11, Server 2016 - 2025 (BDU:2025-00599, уровень опасности по CVSS 3.1 – средний), связанная с ошибками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: установка обновлений из доверенных источников.

27. Уязвимость компонента --dns-updown программного обеспечения OpenVPN версий от 2.7_alpha1 до 2.7_beta1 (BDU:2025-13551, уровень опасности по CVSS 3.1 – высокий), связанная с непринятием мер по нейтрализации специальных элементов при обработке аргументов --dns и --dhcp-option. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

Компенсирующие меры: минимизировать пользовательские привилегии; отключить (удалить) неиспользуемые учетные записи пользователей.

28. Уязвимость объектов QuerySet и Q программной платформы для разработки веб-приложений Django версий от 4.2 до 4.2.26, от 5.1 до 5.1.14, от 5.2 до 5.2.8 и 6.0 на операционной системе РЕД ОС 7.3 (BDU:2025-13913, уровень опасности по CVSS 3.1 – критический), связанная с непринятием мер по защите структуры запроса SQL при обработке аргумента с ключевым словом _connector. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть и изменить защищаемую информацию.

Способ устранения уязвимости: установка обновлений из доверенных источников.

Компенсирующие меры: использовать средства резервного копирования для обеспечения возможности восстановления системы после эксплуатации уязвимости; ограничить доступ из внешних сетей.

29. Уязвимость обработчика CGI-запросов панели управления хостингом Webmin в операционной системе РЕД ОС 7.3 (BDU:2024-11622, уровень опасности по CVSS 3.1 – критический), связанная с ошибками при обработке входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код с root-привилегиями.

Способ устранения уязвимости: установка обновлений из доверенных источников.

Компенсирующие меры: минимизировать пользовательские привилегии; отключить (удалить) неиспользуемые учетные записи пользователей.

30. Уязвимость сценария password_change.cgi панели управления хостингом Webmin и веб-интерфейса для unix-подобных систем Usermin версии 2.100 в операционной системе РЕД ОС 7.3 (BDU:2024-08762, уровень опасности по CVSS 3.1 – средний), связанная с недостатками механизма формирования отчетов об ошибках. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, реализовать атаку методом «грубой силы» (brute force).

Компенсирующие меры: отключить (удалить) неиспользуемые учетные записи пользователей; минимизировать пользовательские привилегии; использовать надежные пароли в соответствии с принятой в организации парольной политикой.

31. Уязвимость виртуального сервера «1С-Битрикс: Виртуальная машина» (VMBitrix) версий до 9.0.5 (BDU:2025-04539, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками разграничения доступа. Эксплуатация

уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии до уровня root.

Способ устранения уязвимости: обновление программного обеспечения.

32. Уязвимость обработчика JavaScript-сценариев V8 браузера Google Chrome версий до 142.0.3595.90, до 142.0.7444.176 операционной системы Astra Linux Special Edition 1.7 (BDU:2025-14497, уровень опасности по CVSS 3.1 – высокий), связанная с ошибками смешения типов данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код с помощью специально созданной HTML-страницы.

Способ устранения уязвимости: обновление программного обеспечения.

33. Уязвимость браузера Mozilla Firefox версий до 124.0.1 в операционных системах Astra Linux Special Edition 1.6, 1.7 и 4.7 (BDU:2024-02305, уровень опасности по CVSS 3.1 – высокий), связанная с выходом операции за границы буфера в памяти в результате некорректной проверки границ на основе диапазона. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код или вызвать отказ в обслуживании.

Способ устранения уязвимости: обновление программного обеспечения.

34. Уязвимость компонента App-Bound Encryption браузеров Google Chrome версий до 142.0.7444.60 и Microsoft Edge версий до 142.0.3595.53 (BDU:2025-14022, уровень опасности по CVSS 3.1 – средний), связанная с ошибками реализации проверки безопасности для стандартных элементов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить доступ к конфиденциальной информации.

Способ устранения уязвимости: обновление программного обеспечения.

35. Уязвимость реализации протокола IPv6 ядра Linux операционных систем Astra Linux Special Edition 1.6, 1.7 и 4.7, РЕД ОС 7.3 (BDU:2023-03643, уровень опасности по CVSS 3.1 – средний), связанная с неконтролируемым потреблением ресурсов при обработке хеш-таблиц. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании путем отправки многочисленных SYN-запросов.

Способ устранения уязвимости: обновление программного обеспечения.

36. Уязвимость компонента Core программного средства виртуализации Oracle VM VirtualBox (BDU:2025-13299 (CVE-2025-62641), уровень опасности по CVSS 3.1 – высокий), связанная с недостатками разграничения доступа.

Эксплуатация уязвимости может позволить нарушителю получить полный контроль над приложением.

Способ устранения уязвимости: обновление программного обеспечения.

37. Уязвимость функции защиты данных BitLocker операционных систем Microsoft Windows версий 10, 11, Server 2016 - 2025 (BDU:2024-00341, уровень опасности по CVSS3.1 – средний), связанная с обходом функции безопасности. Эксплуатация уязвимости может позволить нарушителю обойти существующие ограничения безопасности.

Способ устранения уязвимости: установка обновлений из доверенных источников.

38. Уязвимость почтового сервера Microsoft Exchange Server операционных систем Microsoft Windows версий Server 2013 - 2019 (BDU:2021-01120, уровень опасности по CVSS 3.1 – высокий), связанная с недостаточной проверкой вводимых данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, перезаписать произвольные файлы в системе.

Способ устранения уязвимости: установка обновлений из доверенных источников.

39. Уязвимость компонента Windows Graphics Component операционных систем Microsoft Windows 11 и Server 2025 (BDU:2025-10072, уровень опасности по CVSS 3.1 – критический), связанная с разыменованием недоверенного указателя. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

40. Уязвимость функции Windows Administrator Protection операционной системы Microsoft Windows 11 (BDU:2025-14074, уровень опасности по CVSS 3.1 – высокий), связанная с использованием ненадежного пути поиска. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: установка обновлений из доверенных источников.

41. Уязвимость компонента DirectX Graphics Kernel операционных систем Microsoft Windows версий 10, 11, Server 2008 - 2025 (BDU:2025-11051, уровень опасности по CVSS 3.1 – средний), связанная с ошибками синхронизации при

использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код.

Способ устранения уязвимости: установка обновлений из доверенных источников.

42. Уязвимость драйвера Windows Cloud Files Mini Filter Driver операционных систем Microsoft Windows версий 10, 11, Server 2019 - 2025 (BDU:2025-15480, уровень опасности по CVSS 3.1 – высокий), связанная с переполнением буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: установка обновлений из доверенных источников.