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 почтового сервера Microsoft Exchange Server 2013-2019 г (BDU:2022-06033, уровень опасности по CVSS 3.1 — критический), связанная с ошибками управления генерацией кода. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения уязвимости: Организационные меры.

Компенсирующие меры:

- выполнение следующих шагов:

1. Открыть диспетчер IIS.

2. Развернуть веб-сайт по умолчанию.

3. Выбрать «Автообнаружение».

4. В представлении функций нажать «Перезаписать URL».

5. На панели «Действия» справа нажать «Добавить правила».

6. Выбрать «Блокировка запроса» и нажать «ОК».

7. Добавить строку «.*autodiscover\.json.*\@.*Powershell.*» (без кавычек) и нажать «ОК».

8. Развернуть правило и выбрать правило с шаблоном «.*autodiscover\.json.*\@.*Powershell.*» и нажать «Изменить» в разделе «Условия».

Изменить ввод условия с {URL} на {REQUEST_URI};

- блокировка HTTP-портов 5985 и 5986.

Для проверки компрометации сервера запустить следующую команду PowerShell:

Get-ChildItem -Recurse -Path -Filter "*.log" | Select-String -Pattern 'powershell.*autodiscover\.json.*\@.*200'

2. Уязвимость подсистемы Collaborative Translation Framework (CTFMON) операционных систем Windows версий 10-11, Windows Server 2012-2025 (BDU:2026-08062, уровень опасности по CVSS 3.1 — высокий), связанная с некорректным определением символических ссылок перед доступом к файлу. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения уязвимости: обновление программного обеспечения.

3. Уязвимость почтового сервера Microsoft Exchange Server версий 2016-2019 (BDU:2026-08295, уровень опасности по CVSS 3.1 — высокий), связанная с недостаточной проверкой запросов на стороне сервера. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

Способ устранения уязвимости: обновление программного обеспечения.

4. Уязвимость сетевого компонента skbuff ядра операционных систем Ubuntu, Debian GNU/Linux 11-13 (BDU:2026-08879, уровень опасности по CVSS 3.1 — высокий), связанная с недостаточным контролем ресурса в период его существования. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения: Обновление программного обеспечения.

5. Уязвимость функции prime_handle_to_fd компонента ivpu ядра операционной системы Debian GNU/Linux 13 (BDU:2026-08889, уровень опасности по CVSS 3.1 — высокий), связанная с возможностью использования памяти после освобождения. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

Способ устранения: Обновление программного обеспечения.

6. Уязвимость функций i8042_probe() и i8042_remove() модуля drivers/input/serio/i8042.c драйвера устройств ввода ядра операционной системы Ubuntu 16-22, Debian GNU/Linux 11 (BDU:2026-03970, уровень опасности по CVSS 3.1 — средний), связанная с разыменованием нулевого указателя. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

Способ устранения: Обновление программного обеспечения.

7. Уязвимость системы управления базами данных РЕД ОС 7.3 - 8.0 (BDU:2026-07740, уровень опасности по CVSS 3.1 — критический), связанная с

неверным ограничением имени пути к каталогу. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Способ устранения: Обновление программного обеспечения.

8. Уязвимость Apache Jserv Protocol - коннектора сервера приложений Debian GNU/Linux 9, Astra Linux Special Edition 1.6 (BDU:2020-00937, уровень опасности по CVSS 3.1 — критический), связанная с ошибками при обработке входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

9. Уязвимость функции soup_date_time_to_string() библиотеки доступак HTTP серверам Astra Linux Special Edition 1.8 (BDU:2026-02735, уровень опасности по CVSS 3.1 — высокий), связанная с чтением за допустимыми границами буфера данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить доступ к конфиденциальным данным.

Способ устранения: Обновление программного обеспечения.

10. Уязвимость реализации сетевого протокола Server Message Block (SMBv3) операционных систем Windows 10, Windows Server (BDU:2020-01005, уровень опасности по CVSS 3.1 — высокий), связанная с некорректной обработкой запросов с использованием алгоритма сжатия данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код при помощи специально сформированного пакета.

Способ устранения: Обновление программного обеспечения.

11. Уязвимость драйвера HTTP.sys операционных систем Windows 10, Windows 11, Windows Server (BDU:2026-08063, уровень опасности по CVSS 3.1 — высокий), связанная с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

Способ устранения: Обновление программного обеспечения.

12. Уязвимость Защитника Microsoft 10-11, Microsoft Malware (Windows Defender) операционных систем Windows (BDU:2026-08019, уровень опасности по CVSS 3.1 — высокий), связанная с ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения: Обновление программного обеспечения.

Компенсирующие меры:

- использование систем обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимости;

- минимизация пользовательских привилегий;

- отключение/удаление неиспользуемых учётных записей пользователей.

13. Уязвимость сервера службы каталогов 389 Astra Linux 1.7 - 4.7 (BDU:2025-12486, уровень опасности по CVSS 3.1 — средний), связанная с раскрытием информации. Эксплуатация уязвимости позволяет нарушителю получить доступ к конфиденциальным данным.

Способ устранения: Обновление программного обеспечения.

14. Уязвимость функции nft_map_catchall_activate() компонента nf_tables ядра операционной системы Ubuntu 20.04 - 25.10, Debian GNU/Linux 11 - 13, Astra Linux 1.7, 1.8 (BDU:2026-08031, уровень опасностипо CVSS 3.1 — высокий), связанная с использованием памяти послеее освобождения. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

Способ устранения: Обновление программного обеспечения.

15. Уязвимость модуля обработки заголовков HTTP/2 веб-сервера Apache HTTP Windows Server 2025 (BDU:2026-07789, уровень опасности по CVSS 3.1 — высокий), связанная с неограниченным распределением ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

Способ устранения: Обновление программного обеспечения.

Компенсирующие меры:

- ограничение возможности использования протокола HTTP/2 с помощью строки в основном конфигурационном файле (httpd.conf) или во входящем в комплект конфигурационном файле;

- введение ограничений на максимальное количество заголовков и размер полей в одном запросе.

16. Уязвимость диспетчера очереди печати Windows Print Spooler операционной системы Windows 8.1 - 11, Windows Server 2012 - 2022 (BDU:2022-06785, уровень опасностипо CVSS 3.1 — высокий), связанная с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

Способ устранения: Обновление программного обеспечения.