www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

ТОП/АНТИ-ТОП «страшилок» сентября

Какие уязвимости реально опасны для Рунета

Привет, сисадмины и блу-тимы! 👋

В сегодняшнем списке собрали самые громкие CVE месяца — расскажем, кто реально опасен, а кто просто лает, но не кусает. Не паникуем, патчим и держим руку на логах.

Исследования, приведённые в статье, выполнялись исключительно на уровне внешнего периметра в сети Интернет и могут выявлять только те векторы и артефакты, которые доступны извне (публичные сервисы, открытые порты, публичные конфигурации и метаданные). Эти результаты не отображают состояние внутренней инфраструктуры, сетевой сегментации, конфигураций на хостах, контроля привилегий или телеметрии. Для корректной и полной оценки уровня безопасности нужно обязательно провести внутренние аудирование.

HOT-HOT! ТОП-5 уязвимостей по охвату в Рунете

1. GitLab / Вебхук-шпиён (CVE-2025-6454)

CVSS: 8.8 | KEV: нет | Real World Danger: 2.0

Масштаб: На радарах СКИПА фиксируется ~30.000 активных инстансов GitLab в Рунете. Из них ~37% потенциально уязвимы.

Суть: Уязвимость позволяет аутентифицированному пользователю инициировать внутренние запросы через прокси и внедрять SSRF в заголовки-вебхуков.

Что по факту: Старые инстансы под риском CI/CD атак. Патч вышел в релизе 18.3.2. — обновись прямо сейчас!

Вердикт: Массовая поверхность атаки — апдейт обязателен. Смотрим в оба за вебхуками в средах разработки и CI.

2. UMI CMS / XSS-ловушка для админов (BDU:2025-08683)

CVSS: 9.1 | KEV: нет

Масштаб: По данным СКИПА в Рунете работает ~20.000 активных инстансов UMI CMS. ~2.000 из них уязвимы.

Описание: Некорректная валидация веб-страниц позволяет внедрять XSS через специально подготовленный файл, захватывать админ-сессии и выполнять вредоносный JS в контексте панели управления.

Что по факту: Большая база инсталляций + солидный пул уязвимых экземпляров = привлекательный вектор для целевых атак, мошенничества с аккаунтами и дальнейшей компрометации сайтов. Несмотря на небольшое количество упоминаний, баг простой и работающий.

Вердикт: Высокий приоритет для аудита UMI-инстансов, патчинга и внедрения правил очистки/контроля контента.

3. PARTS SOFT CMS / Тук-тук! Кто в системе живет? (BDU:2025-05287 / BDU:2025-05286)

BDU:2025-05286 — CVSS: 6.1 | KEV: нет BDU:2025-05287 — CVSS: 7.5 | KEV: нет

Масштаб: На радарах СКИПА наблюдаем ~5.000 инстансов PARTS SOFT CMS. Пока патча нет — потенциально все уязвимы.

Описание: Различия в ответах сервера позволяют злоумышленнику осуществлять перебор (enumeration) пользователей. Это раскрывает конфиденциальную информацию и упрощает атаки password-spraying и фишинг. Перебор ID может использоваться для целенаправленной CSRF-эксплуатации.

Что по факту: Широкое наличие в открытой сети и отсутствие исправления — классика для автоматизированных массовых атак, особенно в связке с фишинг-кампаниями.

Вердикт: Мониторим, ставим ограничение запросов, ставим WAF/ratelimit — пока патча нет, компенсируем.

4. TrueConf Server / Онлайн-конференция для эксплойтов (BDU:2025-10114 / BDU:2025-10115 / BDU:2025-10116)

BDU:2025-10114 — CVSS: 7.5 | KEV: нет BDU:2025-10115 — CVSS: 7.5 | KEV: нет BDU:2025-10116 — CVSS: 9.8 | KEV: нет

Масштаб: TrueConf — одна из самых популярных платформ ВКС в РФ. По данным СКИПА, в Интернете доступно несколько тысяч установок, более 80% из них потенциально уязвимы (один

хост может быть затронут всеми тремя уязвимостями). На данный момент не наблюдается доступных публичных эксплойтов.

Описание: В августе найдены три уязвимости в TrueConf Server; все подтверждены вендором и исправлены.

Что по факту: Платформа широко распространена, процент уязвимых инстанций высокий — если не применили апдейты, можно получить массовые проблемы с конфиденциальностью и доступностью.

Вердикт: Критический приоритет для операторов ВКС — массовый патчинг и проверка инсталляций обязательны.

5. Cisco IOS/IOS XE / Открытый SNMP ≠ «всё ок» (CVE-2025-20352)

CVSS: 7.7 | KEV: нет | Real World Danger: 4.0

Масштаб: СКИПА фиксирует >30 000 устройств с SNMP v1/v2c в Рунете. Из них ≈1 700 выглядят потенциально уязвимыми к CVE-2025-20352.

Описание: Переполнение стека в подсистеме SNMP Cisco IOS/IOS XE. Для эксплуатации требуются валидные SNMP-учётки. При низких правах возможен DoS (перезагрузка). На IOS XE при повышенных правах возможен RCE через специально сформированные SNMP-пакеты. Уязвимость имеет признаки 0-day — используется злоумышленниками.

Что по факту: Если у вас открыт SNMP и/или скомпрометированы SNMP-учётные записи —риск растет. Операторам сети срочно проверить SNMP-доступность, применить фильтрацию и обновления, а также отозвать/сменить credentials.

Вердикт: Критично для сетевой инфраструктуры — приоритет для немедленной проверки и мер по снижению риска (фильтрация, обновление, смена учётных данных).

АНТИТОП-5

1. FreePBX / Купи модуль, взломы в подарок (CVE-2025-57819)

CVSS: 10 | KEV: да | Real World Danger: 2.0 | Упоминания СКИПА: 25+

Описание: Уязвимость в FreePBX (терминалы 15/16/17) позволяет обходить защиту пользовательских данных и получить неавторизованный доступ к админке, что теоретически даёт возможность манипуляций с базой данных и удалённого выполнения кода. Вендор выпустил фиксы.

Что по факту: Для эксплуатации нужен платный модуль EndPoint Manager. Публичные PoC/шаблоны нестабильны и экзотичны (техники типа time-based / union-based).

Вердикт: Серьёзная уязвимость по описанию и с KEV в истории, но риск для Рунета локален и специфичен.

2. Telerik Report Server / Читать отчеты без смс и регистрации (CVE-2024-4358)

CVSS: 9.8 | KEV: да | Real World Danger Score: 5.0 | Упоминания СКИПА: 10+

Описание: В старых сборках Telerik Report Server на IIS возможен обход аутентификации, что даёт неавторизованному атакующему доступ к ограничённой функциональности и потенциальной эскалации.

Что по факту: Уязвимость серьёзная, KEV есть, но продукт в Рунете встречается редко — видимых хостов мало.

Вердикт: Опасна по сути, но для РФ-сегмента не популярна. Патчите, если есть.

3. BIG-IP Next Central Manager / Слишком откровенный API (CVE-2024-26026)

CVSS: 9.8 | KEV: не подтверждено | Real World Danger Score: 2.0 | Упоминания СКИПА: 5+

Описание: SQL-инъекция в API BIG-IP Next Central Manager может позволить атакующему выполнить произвольные запросы к базе данных.

Что по факту: Интерфейсы видны преимущественно в локалках; публичных экземпляров в интернете почти не найдено; демонстрационной среды/экземпляра в интернет-пространстве эксперты не обнаружили.

Вердикт: Теоретически критично, но в Рунете ПО практически не представлено — риск крайне низкий.

4. SAP NetWeaver на IBM i-series / Проверка подлинности (CVE-2025-42958)

CVSS: 9.1 | KEV: не подтверждено | Real World Danger Score: 2.0 | Упоминания СКИПА: < 5

Описание: Недостаточная проверка подлинности в приложении на IBM i-series даёт возможность неавторизованным пользователям с высокими привилегиями работать с конфиденциальными данными и административными функциями.

Что по факту: Критичный профиль, но продукт крайне редок в Рунете. Уход вендора с рынка РФ может осложнить апдейты, но публичных уязвимых хостов не видно.

Вердикт: Серьёзная уязвимость для тех, у кого есть такой актив, но массовой угрозы в Рунете нет.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

5. GitHub Enterprise Server / Админ играет в root-рулетку (CVE-2024-2469)

CVSS: 7.2 | KEV: не подтверждено | Real World Danger Score: 2.0 | Упоминания СКИПА: < 5

Описание: Уязвимость позволяла злоумышленнику с ролью администратора выполнить код и получить root-доступ через SSH. Исправлено в рядах релизов.

Что по факту: GitHub Enterprise в РФ-сегменте встречается редко; публичных инстансов с подтверждённой уязвимостью не обнаружено.

Вердикт: Технически серьёзно, но для отечественной инфраструктуры — практически неактуальна.

Выводы

Среди этих CVE есть как действительно подтверждённые и опасные (KEV), так и те, которые на бумаге выглядят страшно, но в Рунете встретить их почти нереально. Правила просты:

- Знайте свой сетевой периметр! Патчите то, что реально активно у вас в сети.
- KEV = рэд флэг. Если там есть эксплойты, то действуйте.
- Даже редкие уязвимости требуют внимания