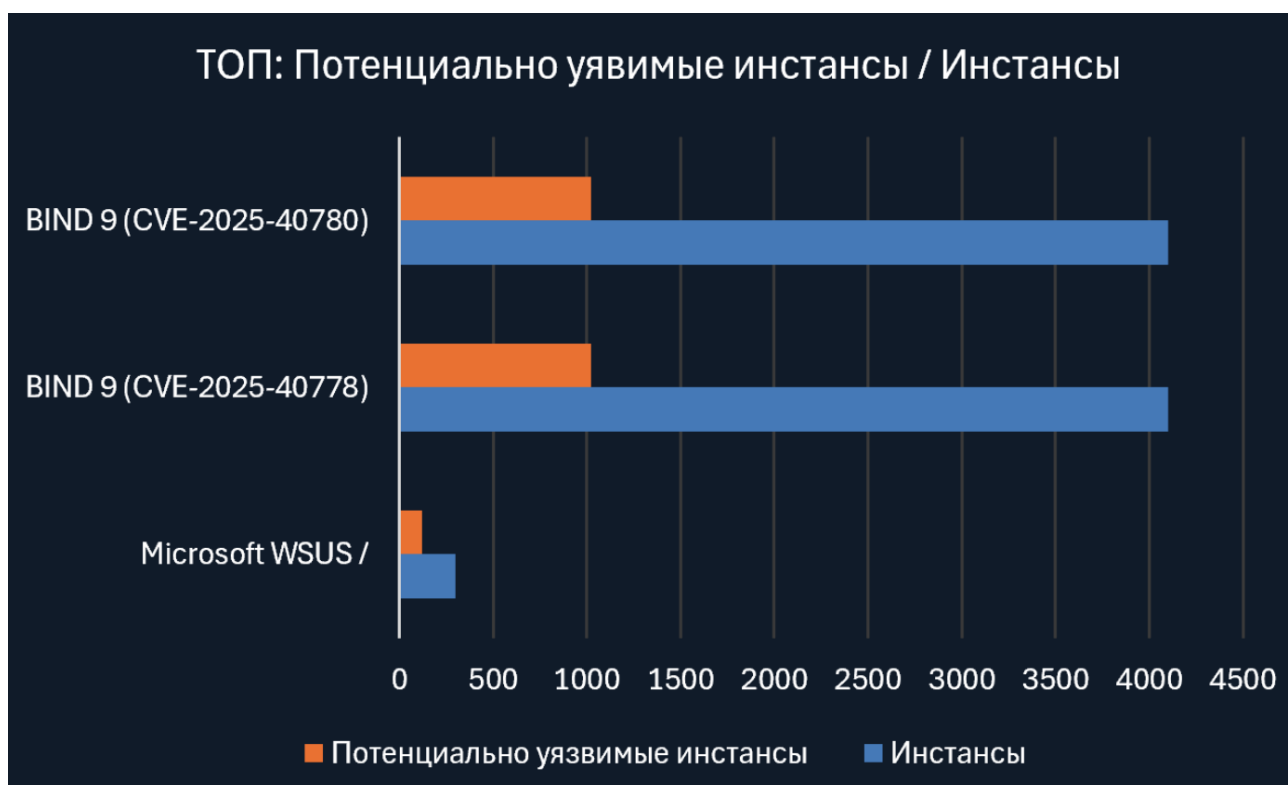


## РУНЕТ В СТРАНЕ КОШМАРОВ: ТОП/АНТИТОП УЯЗВИМОСТЕЙ ОКТЯБРЯ

Как вы провели Хэллоуин? Вот мы в СайберОК качественно повеселились и попугались, ведь наши эксперты-охотники на привидений до самого рассвета рыскали по внешнему периметру Рунета и вытаскивали на свет главных монстров октября – как новых, так и хорошо забытых старых.

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.

### ТОП: Высокий риск + высокий охват в Рунете



## 1. RCE в Microsoft WSUS / Обновить нельзя эксплуатировать (CVE-2025-59287)

CVSS: 9.8 | KEV: да

**Масштаб:** На радарх СКИПА мы наблюдаем ~300 инстансов Microsoft WSUS SimpleAuthWebService, из которых уязвимы около 40%.

**Описание:** Критическая уязвимость RCE в службах обновления Microsoft Windows Server (WSUS). Проблема вызвана небезопасной десериализацией данных AuthorizationCookie с помощью BinaryFormatter в методе EncryptionHelper.DecryptData(). Уязвимость позволяет злоумышленнику без аутентификации выполнить удаленный код с привилегиями SYSTEM, отправив вредоносные зашифрованные файлы cookie на конечную точку GetCookie().

**Что по факту:** Критическое ПО, успешные кейсы эксплуатации уязвимости в дикой природе уже зафиксированы.

**Вердикт:** Серьёзная уязвимость с KEV, срочно обновить.

1 угроза из 13 источников

Опубликовано: 14.10.2025 Обновлено: 28.10.2025 Последнее упоминание: 31.10.2025 Внедрено 28.10.2025, 13:41 E63: 16.10-29.10

CVE-2025-59287 EPSS 0.094 CybVSS 0.0 RWDS - 66 1 0 5 4

Десериализация ненадежных данных в службе обновления Windows Server позволяет неавторизованному злоумышленнику выполнить код по сети.

Версия	Вектор	BS	TS	ES	ExS	IS
CVSS 3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	9.8	9.8	3.9	5.9

cpe:2.3:o:microsoft:windows\_server\_2012-\*:\*:\*:\*:\*:\* + ещё 477

**KEV** microsoft microsoft:windows\_server\_2012 microsoft:windows\_server\_2016 microsoft:windows\_server\_2019 microsoft:windows\_server\_2022 microsoft:windows\_server\_2022\_23h2 microsoft:windows\_server\_2025 + ещё 6

1 угроза из 13 источников

## 2. BIND 9 / Cache Poisoning (CVE-2025-40778)

CVSS: 8.6 | KEV: нет

**Масштаб:** На радарх СКИПА мы наблюдаем ~4.100 инстансов BIND-9, из которых уязвимы около 25%.

**Описание:** При определённых обстоятельствах BIND недостаточно валидирует записи в ответах, что позволяет злоумышленнику внедрять поддельные данные в кэш.

**Что по факту:** Публичный PoC доступен, злоумышленник способен внедрять поддельные записи в кэш уязвимого резолвера, что приведёт к подмене DNS-ответов для всех его клиентов (редирект трафика, подмена адресов сервисов и т.п.). Потенциально масштабная атака на незащищённые инстансы.

**Вердикт:** Серьёзная уязвимость — обновить BIND немедленно. До патча: ограничить рекурсивный доступ (ACL), запретить рекурсию на публичных серверах, включить/проверить DNSSEC на критичных зонах, мониторить нестандартные RRset в кэше и логи ответов.

### 3. BIND 9 / Повышаем градус эксплуатации (CVE-2025-40780)

CVSS: 8.6 | KEV: нет

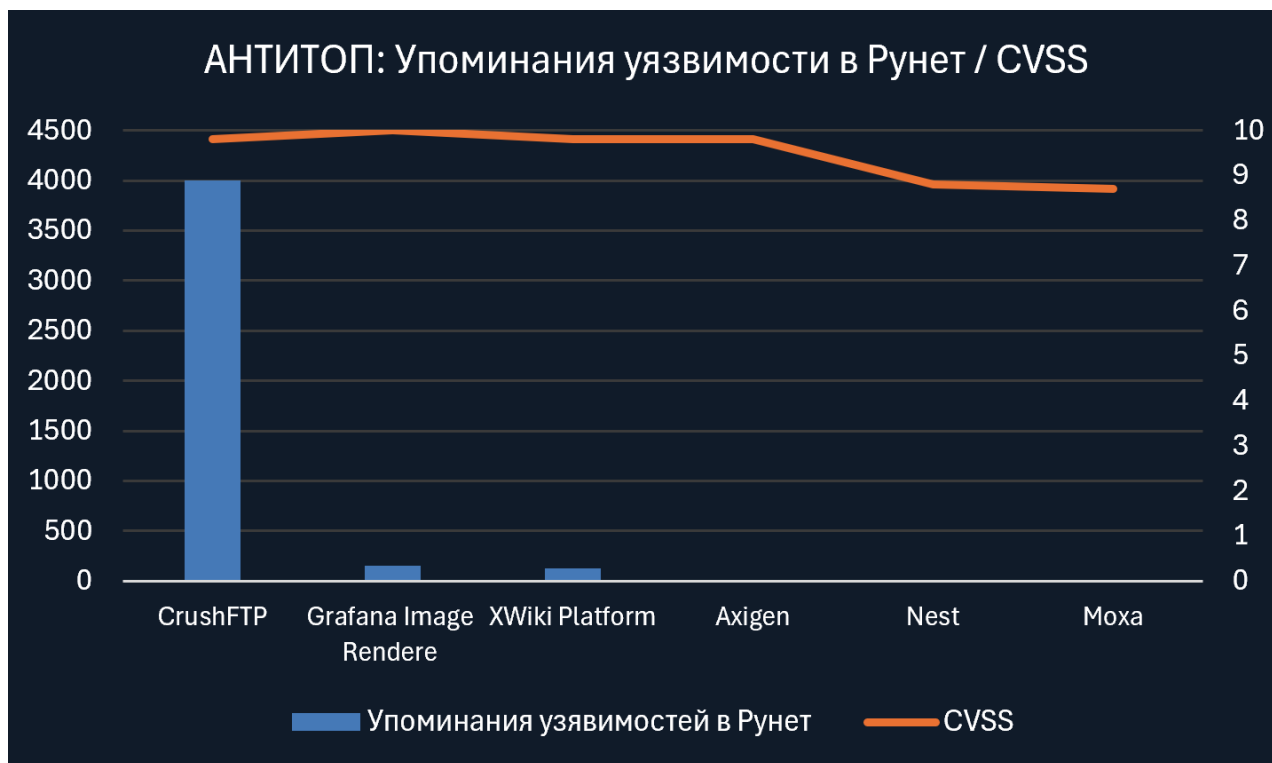
**Масштаб:** На радарх СКИПА мы наблюдаем ~4.100 инстансов BIND-9, из которых уязвимы около 25%.

**Описание:** Ослабление энтропии генератора псевдослучайных значений, используемого для формирования transaction ID и source port. Сужение пространства возможных комбинаций значительно повышает вероятность успешного угадывания полей, по которым резолвер сопоставляет ответы с запросами.

**Что по факту:** В сочетании с уязвимостью в обработке unsolicited RRs (CVE-2025-40778) сниженная случайность делает приёмы форженных ответов гораздо более надёжными — публичный PoC показывает практическую пригодность этой техники. Риск — массовая подмена кэша при таргетинге уязвимых резолверов.

**Вердикт:** Критично — поставить патч как можно скорее. До патча: по возможности ограничить исходящие/входящие порты, использовать NAT/порт-рандомизацию на сетевом уровне, включить DNSSEC, отслеживать аномалии в совпадениях transaction ID/port и рассмотреть перевод критичных клиентов на надёжные внешние резолверы.

## АНТИТОП: Высокий риск + низкий охват в Рунете



## 1. CrushFTP / Гонка за креслом admin (CVE-2025-31161)

CVSS: 9.8 | KEV: да | Упоминания СКИПА: 50+

**Описание:** CrushFTP версии до 10.8.4 / 11.x до 11.3.1 содержат уязвимость, позволяющую обойти аутентификацию и получить контроль над учётной записью crushadmin (если не используется прокси в DMZ). В методе авторизации AWS4-HMAC (S3-совместимой) в HTTP-компоненте FTP-сервера есть состояние гонки: сервер сначала вызывает login\_user\_pass() без запроса пароля — в этот момент сессия проходит проверку HMAC и считается аутентифицированной, а позднее сервер повторно проверяет пользователя.

**Что по факту:** В Рунете ~4000 экземпляров, есть публичный PoC и poc1e1-шаблоны, но массовых кейсов эксплуатации подтвердить не удалось.

**Вердикт:** Серьёзная уязвимость, однако активность в Рунете не зафиксирована массово.

Угрозы &gt; CVE-2025-31161



CVE-2025-31161

<https://nvd.nist.gov/vuln/detail/CVE-2025-31161>Загружено 03.04.2025, 23:44  
Обновлено 28.10.2025, 15:53  
Последнее упоминание 06.05.2025, 13:02

Подробности Упоминания Конфигурации (CVEs) Эксплоиты История

Период упоминаний: Все упоминания

reddit   🔥 top 10 trending cves (06/05/2025)	06.05.2025, 13:02
reddit   🔥 top 10 trending cves (05/05/2025)	05.05.2025, 13:07
twitter   rt @darkwebinforme: 🚩cve-2025-31161: authentication bypass vulnerability in crushftp credit: https://t.co/lfshrgpkup exploit: https://t.c...	05.05.2025, 11:17
twitter   rt @darkwebinforme: 🚩cve-2025-31161: authentication bypass vulnerability in crushftp credit: https://t.co/lfshrgpkup exploit: https://t.c...	05.05.2025, 10:22

## 2. Axigen / Обход 2FA (CVE-2023-23566)

CVSS: 9.8 | KEV: нет | Упоминания СКИПА: 5+

**Описание:** Уязвимость в Axigen 10.3.3.52 даёт возможность обхода двухэтапной аутентификации, что позволяет злоумышленнику получить доступ к ящику при подключении учётной записи к стороннему веб-почтовому сервису.

**Что по факту:** Уязвимости подвержена версия приложения 10.3.3.52. В Рунете инстансы с данной версией не обнаружены.

**Вердикт:** Опасна по сути, но для РФ-сегмента не актуальна.

## 3. Nest RCE / Небезопасная песочница (CVE-2025-54782)

CVSS: 8.8 | KEV: нет | Упоминания СКИПА: 10+

**Описание:** В версиях ≤0.2.0 в пакете @nestjs/devtools-integration была обнаружена критическая уязвимость удалённого выполнения кода (RCE). При активации пакет предоставляет доступ к локальному HTTP-серверу разработки с конечной точкой API, использующей небезопасную песочницу JavaScript.

**Что по факту:** В РУ сегменте не обнаружено активных инстансов данного ПО.

**Вердикт:** Крайне низкий риск для Рунета.

Угрозы &gt; CVE-2025-54782



## CVE-2025-54782

<https://nvd.nist.gov/vuln/detail/CVE-2025-54782>Загружено 06.08.2025, 10:07  
Обновлено 28.10.2025, 15:56  
Последнее упоминание 10.10.2025, 03:07

[Подробности](#)
[Упоминания](#)
[Конфигурации \(CPEs\)](#)
[Эксплоиты](#)
[История](#)

Ru En

Nest — это фреймворк для создания масштабируемых серверных приложений Node.js. В версиях 0.2.0 и ниже в пакете @nestjs/devtool-integration была обнаружена критическая уязвимость удалённого выполнения кода (RCE). При активации пакет предоставляет доступ к локальному HTTP-серверу разработки с конечной точкой API, использующей небезопасную песочницу JavaScript (реализация типа safe-eval). Из-за некорректной песочницы и отсутствия защиты от кросс-доменных источников любой вредоносный веб-сайт, посещённый разработчиком, может выполнить произвольный код на его локальном компьютере. Пакет добавляет конечные точки HTTP к локально работающему серверу разработки NestJS. Одна из этих конечных точек, /inspector/graph/interact, принимает входные данные JS ON, содержащие поле кода, и выполняет предоставленный код в песочнице Node.js vm.runInNewContext. Это исправлено в версии 0.2.1.

## Ссылки

Ссылка	Ресурс
<a href="https://socket.dev/blog/nestjs-rce-vuln">https://socket.dev/blog/nestjs-rce-vuln</a>	
<a href="https://nodejs.org/api/vm.html">https://nodejs.org/api/vm.html</a>	
<a href="https://github.com/nestjs/nest/security/advisories/GHSA-85cg-cmq5-qjm7">https://github.com/nestjs/nest/security/advisories/GHSA-85cg-cmq5-qjm7</a>	
<a href="https://github.com/JLLeitschuh/nestjs-typescript-starter-w-devtools-integration">https://github.com/JLLeitschuh/nestjs-typescript-starter-w-devtools-integration</a>	

Развернуть

Статус **Исследование прекращено**

Ссылка на задачу #2663

Исследование прекращено с 10.10.2025, 10:15

Исследователь

Milestone

Base score (CVSS 4.0) **9.4**EPSS **0.142**CybVSS **0.0**Real world danger score **-**

CVSS 4.0 CVSS 3.1

CVSS-4.0/AV:A/AC:L/ATAU/PR:N/UI:N/A/C:H/V:H/A:N/SC:H/SI:Z/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MV:X/MVA:X/MSC:X/MS:X/MSA:X/SX:ALX/RX/LX/REX/UX

## 4. Моха / Админская дверь без замка (CVE-2025-6892)

CVSS: 8.7 | KEV: нет | Упоминания СКИПА: 5+

**Описание:** В сетевых устройствах безопасности и маршрутизаторах Моха обнаружена уязвимость, связанная с некорректной авторизацией. Изъян в механизме аутентификации API позволяет получить несанкционированный доступ к защищённым конечным точкам API, включая те, которые предназначены для выполнения административных функций. Эта уязвимость может быть эксплуатирована после входа в систему аутентифицированного пользователя, поскольку система не может должным образом проверить контекст сеанса и не ограничивает привилегии должным образом.

**Что по факту:** Не удалось оценить распространённость в Рунете.

**Вердикт:** Крайне низкая вероятность активной эксплуатации в РУ сегменте.

## 5. Grafana Image Renderer RCE / Хардкод ключик (CVE-2025-11539)

CVSS: 10 | KEV: нет | Упоминания СКИПА: 5+ | Cybvss: 54.6\*

**Масштаб:** По данным СКИПА в Рунете работает ~150 активных инстансов, на момент исследования 100% из них уязвимы.

**Описание:** Grafana Image Renderer уязвим к удалённому выполнению кода из-за уязвимости записи произвольного файла. Это связано с тем, что конечная точка /render/csv не проходит проверку параметра filePath, что позволяет злоумышленнику сохранить общий объект в произвольном месте, а затем загрузить его процессом Chromium. Экземпляры уязвимы, если токен по умолчанию («authToken») не изменён или известен злоумышленнику.

**Что по факту:** Так как токен можно легко получить из исходного кода приложения, необходимо срочно изменить «authToken» на отличный от стандартного значения.

**Вердикт:** В Рунете такие экземпляры встречаются нечасто и не задерживаются на радаре.

\* *CybVSS – CyberOK Vulnerability Scoring System – метрика, разработанная нашими экспертами. Используется для быстрой оценки уязвимости на основе многих данных о ней.*

The screenshot displays a search interface for the URL `http.body:"grafana-image-renderer"`. It shows a list of results categorized by location (Города) and organization (Организации). Two detailed view panels are visible:

- Panel 1 (TCP / HTTP / 8081):** Shows a connection from Russia (ASN) on 31.10.2025 at 12:46. The banner is `Nodejs`. The response is `HTTP/1.1 200 OK` with headers: `Connection: close`, `Content-Length: 22`, `Content-Type: text/html; charset=utf-8`, `Date: Fri, 31 Oct 2025 09:46:28 GMT`, `Etag: W/"16-NipK48ud1bhsozqKdmj9bMnwGTg"`, and `X-Powered-By: Express`.
- Panel 2 (TCP / HTTP / 32772):** Shows a connection from Russia, Moscow (ASN) on 31.10.2025 at 12:38. The banner is `Nodejs`. The response is `HTTP/1.1 200 OK` with headers: `Connection: close`, `Content-Length: 22`, `Content-Type: text/html; charset=utf-8`, `Date: Fri, 31 Oct 2025 09:37:53 GMT`, and `Etag: W/"16-NipK48ud1bhsozqKdmj9bMnwGTg"`.

## 6. XWiki Platform / RCE (CVE-2025-24893)

CVSS: 9.8 | KEV: да | Упоминания СКИПА: 30+

**Описание:** Уязвимость в XWiki реализуется через эндпоинт SolrSearch и позволяет любому пользователю выполнить произвольный код на хосте — без необходимости привилегий. Причина — недостаточная санитизация и/или некорректная обработка пользовательских параметров при формировании запросов/шаблонов для поискового компонента (Solr/механизмы шаблонизации).

**Что по факту:** В октябре был всплеск упоминаний уязвимости в публичных источниках. Эксперты СайберОК рассмотрели данную уязвимость в марте 2025 года: на момент исследования было приблизительно 7–8% уязвимых экземпляров.

На сегодняшний день СКИПА видит примерно ~130 активных хостов с данным ПО в Рунете.

**Вердикт:** Уязвимость крайне опасная, но низкая распространённость в Рунете делает её менее приоритетной с точки зрения массовой эксплуатации — однако для подверженных экземпляров обновление и внедрение компенсирующих мер остаются обязательными.

## Выводы

Может быть самая страшная ночь в году и осталась позади, но уязвимостям сон не введом.

1. Найдите свой сетевой периметр — освятите его светом инвентаризации и патчей.
2. Если по сети ползёт эксплойт — действуйте без промедления, пока тени не окутали ваши сервисы.
3. Даже редкие уязвимости могут ожить в полночь — удавите их прямо в колыбели.

И пусть ваши системы вздохнут спокойно под покровом обновлений.

В нашем [телеграм-канале](#) — кладовая знаний по кибербезопасности и мониторингу внешних атак. Заглядывайте.