КОД ИБ | ИТОГИ 2025

А уязвим ли мессенджер?

Москва, 2025

Исхаков Андрей Юнусович
Andrey Iskhakov

Заместитель начальника управления безопасности инфраструктуры - начальник отдела анализа защищенности инфраструктуры

Deputy Head of the Infrastructure Security Department

А уязвим ли мессенджер?

О чем данный доклад?

Disclamer

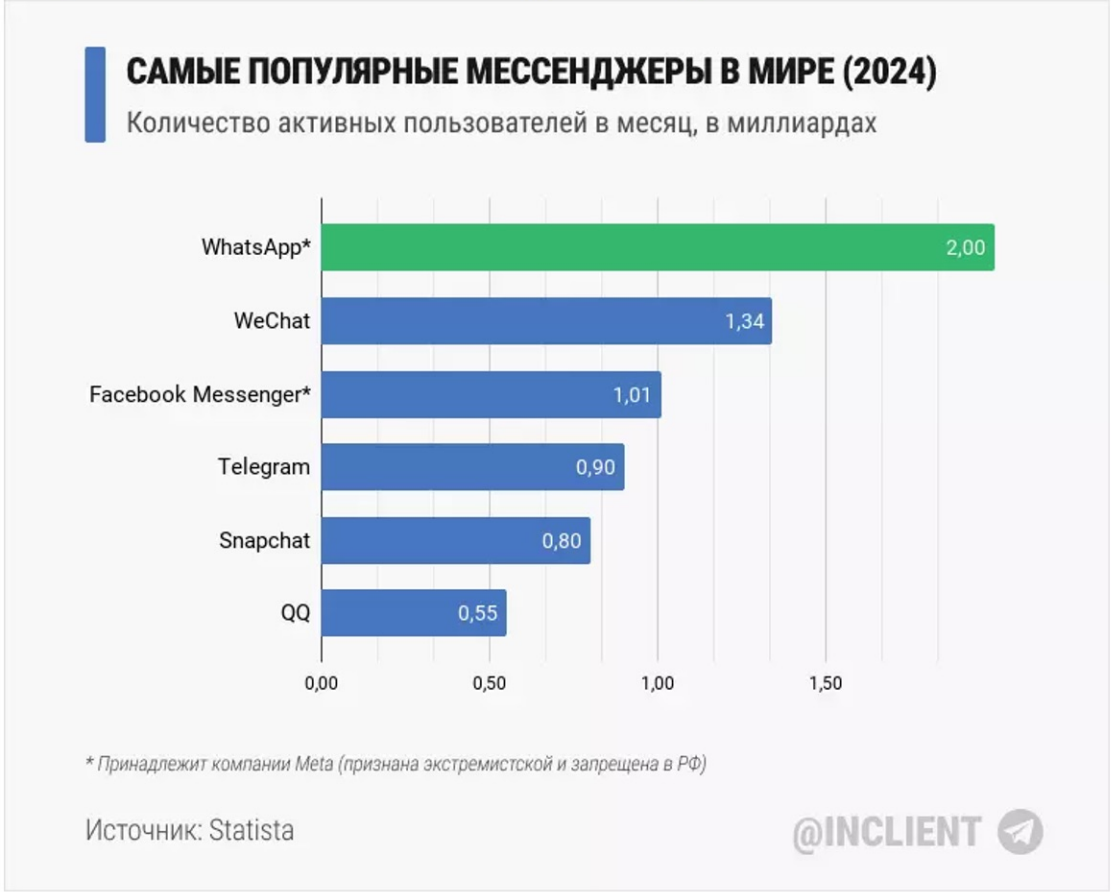
1) Данная презентация не является публикацией результатов проведенного НИР по оценке защищенности известных мессенджеров, а представляет собой консолидацию аналитических сведений об известных уязвимостях.

2) В презентации упоминаются мессенджеры *FB, *WhatsApp — продукты компании Meta, признанной экстремистской и запрещённой в РФ.

История развития мессенджеров

Источник: https://trends.rbc.ru/trends/innovation/624ecb0a9a7947bc23da3640

Текущая статистика (2024)



Так что же с уязвимостями?

Основные классы уязвимостей

Zero-click и RCE

эксплуатация без участия пользователя

Ошибки авторизации и логики

обход проверки доступа

Утечки метаданных

анализ графов коммуникаций

Криптографические уязвимости

ошибки имплементации протоколов

Сторонние приложения и supply-chain

клоны, SDK

Социальная инженерия

фишинг, перехват otp

*WA. Немного статистики (CVE)

Год	CVE	CVE (NVD / MITRE) — примечания
2018	5	CVE-2018-6339 · CVE-2018-6344 · CVE-2018-6349 · CVE-2018-6350 · CVE-2018-20655. Примеры: CVE-2018-6349 (stack-based overflow при приёме звонков (все 5 записей детально описаны в NVD/WhatsApp advisory archive)
2019	8	**CVE-2019-3568** (VOIP stack RCE / Pegasus-related exploitation context documented в расследованиях)· CVE-2019-18426 (WhatsApp Desktop XSS / локальное чтение файлов в паре с iPhone)
2020	14	CVE-2020-1901 – 09 CVE-2020-1886 CVE-2020-1889 CVE-2020-1890 CVE-2020-1891 CVE-2020-1894
2021	5	CVE-2021-24026 · CVE-2021-24027 · CVE-2021-24035 · CVE-2021-24041 · CVE-2021-24042 — критические уязвимости в обработке мультимедиа/вызывной логике/архивах (из NVD). Примеры: CVE-2021-24035 — path traversal при распаковке zip в Android-клиенте; CVE-2021-24042 — out-of-bounds write при звонке.
2022	2	CVE-2022-27492 (integer underflow при парсинге видео) · CVE-2022-36934 (integer overflow -> возможное RCE в видео-звонке). Обе — NVD
2023	2	CVE-2023-38537 и CVE-2023-38538
2024	1	CVE-2024-45607 — incorrect access control в whatsapp-api-js (официальный TypeScript/Server SDK от WhatsApp). Это серверный SDK (official API framework)
2025	3	**CVE-2025-30401** (spoofing / attachment handling — WhatsApp for Windows).
		CVE-2025-30259 (WhatsApp cloud service — crafted PDF / sandbox bypass — NVD).
		CVE-2025-55177 (incomplete authorization for linked device sync — iOS/Mac; попало в CISA/Known Exploited list).

Tg. Немного статистики (CVE)

Год	Количество CVE)	Примеры / основные CVE (NVD ссылки)
2018	6	CVE-2018-17231, CVE-2018-17613, CVE-2018-17780, CVE-2018-20436, CVE-2018-15542, CVE-2018-15543.
2019	3	CVE-2019-10044 (IDN/homograph / multiple clients), CVE-2019-16248 (Delete-for privacy issue), CVE-2019-15514 (info disclosure).
2020	2	CVE-2020-12474 (IDN/visual issues reported), CVE-2020-17448 (file/content handling bypass).
2021	10	Набор уязвимостей, в основном связанные с кастомным форком rlottie (анимированные стикеры): CVE-2021-31315, CVE-2021-31317, CVE-2021-31318, CVE-2021-31319, CVE-2021-31323, CVE-2021-27204, CVE-2021-27351, CVE-2021-30496, CVE-2021-36769, CVE-2021-41861.
2022	2	CVE-2022-43363 (Telegram Web — XSS; CVE помечено как disputed/обсуждаемое в NVD), также есть уязвимость, относящаяся к веб-версии/компонентам.
2023	1	CVE-2023-26818 (macOS / environment variable loading / privilege escalation vectors)
2024	1	CVE-2024-54916 (SharedConfig / auth/session related)

Signal. Немного статистики (CVE)

Год	Кол-во CVE	Примеры / основные CVE (NVD ссылки)
2018	1	CVE-2018-3988 — Signal Android: исчезающие сообщения могли сохраняться (privacy issue).
2020	1	CVE-2020-5753 — Signal: ICE candidates / WebRTC DNS leakage при звонке (Android/iOS).
2022	1	CVE-2022-28345 — Signal iOS: RTLO URI spoofing.
2024	2	CVE-2024-45620 — libsignal-client: integer overflow (bindings). CVE-2024-37474 — Signal Desktop: improper certificate validation.
2025	2	CVE-2025-24903 — libsignal-service-java: heap buffer overflow. CVE-2025-24904 — libsignal-service-java: memory safety issue

Discord. Немного статистики (CVE)

Год	Кол-во CVE	Примеры / основные CVE
2019	1	CVE-2019-20012 — Discord Desktop до 0.0.305: некорректная обработка URL (XSS/command injection).
2020	1	CVE-2020-15174 — Discord Rich Presence SDK: небезопасное десериализ. в RPC (RCE)
2021	2	CVE-2021-21306 — Discord Desktop (Electron auto-update, DLL hijacking). CVE-2021-29447 — Discord Android app: обработка PNG (через библиотеку Skia, но зафиксировано в контексте Discord)
2022	2	CVE-2022-36032 — Discord Desktop: произвольное выполнение кода через IPC. CVE-2022-24783 — Discord API SDK: небезопасное выполнение JS.
2023	1	CVE-2023-33918 — Discord Windows client: небезопасная загрузка библиотек.
2024	1	CVE-2024-27072 — Discord Electron Desktop <0.0.309: обход политики безопасности.

Wire. Немного статистики (CVE)

Год	Кол-во CVE	Примеры / основные CVE (NVD ссылки)
2018	1	CVE-2018-17195 — Wire Android до 3.9.1: утечка конфиденциальных данных через debug logs.
2020	1	CVE-2020-26664 — Wire WebApp <2020-09: XSS в preview ссылок.
2021	2	CVE-2021-40825 — Wire iOS: утечка ключей в журнале. CVE-2021-40826 — Wire Android: небезопасное хранение токенов
2022	1	CVE-2022-31214 — Wire Server: SQL injection в management AP
2023	1	CVE-2023-4969 — Wire Desktop (Electron): небезопасная загрузка библиотек

Matrix / Element.
Немного статистики (CVE)

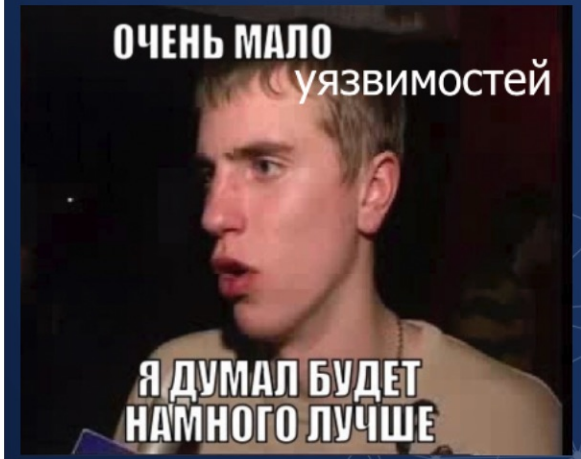
Год	Кол-во CVE	Примеры / основные CVE (NVD ссылки)
2018	2	CVE-2018-17190 — Synapse: XSS в preview ссылок. CVE-2018-17721 — Synapse <0.33.3: SSRF в media repo
2019	1	CVE-2019-5885 — Synapse <0.99.3: DoS через авторизацию
2020	2	CVE-2020-26890 — Synapse: обход авторизации в /_matrix/federation/v1 API CVE-2020-26257 — Element Web <1.7.14: XSS в URL preview.
2021	3	CVE-2021-29433 — Synapse: SSRF в URL preview. CVE-2021-39233 — Element Web/Desktop: XSS в room settings. CVE-2021-41281 — Element iOS: обход шифрования при share-файлах.
2022	2	CVE-2022-39249 — Synapse: DoS через room aliases. CVE-2022-39251 — Element Android <1.4.23: токены в логах.
2023	2	CVE-2023-32323 — Element Web/Desktop: XSS в link previews. CVE-2023-41335 — Synapse: SQL injection в state resolution.
2024	1	CVE-2024-45367 — Synapse federation API: утечка PII в error responses.

Threema. Немного статистики (CVE)

Год	Кол-во CVE	Примеры / основные CVE (NVD ссылки)
2020	1	CVE-2020-26541 — Threema Android <4.51: MITM в WebSocket (недостаточная валидация сертификатов).
2021	1	CVE-2021-33916 — Threema iOS <4.6.3: утечка данных через push-уведомления.
2022	1	CVE-2022-31061 — Threema Web <2.4.3: XSS в обработке сообщений.
2023	2	CVE-2023-45866 — Threema Desktop (Electron): произвольное выполнение кода. CVE-2023-48365 — Threema Gateway API: уязвимость подсистемы аутентификация.

Сводка по всем (CVE)

Год	WhatsApp	Telegram	Signal	Discord	Wire	Matrix/Element	Threema	Итого за год
2018	5	6	1	0	1	2	0	**15**
2019	8	3	0	1	0	1	0	**13**
2020	14	2	1	1	1	2	1	**22**
2021	5	10	0	2	2	3	1	**23**
2022	2	2	1	2	1	2	1	**11**
2023	2	1	0	1	1	2	2	**9**
2024	1	1	2	1	0	1	0	**6**
2025	3	0	2	0	0	0	0	**5**
Всего	**40**	**25**	**7**	**8**	**6**	**13**	**5**	**104**



Выводы

- **Обработка медиаконтента — частый вектор.**
  Большая часть критичных CVE (RCE/DoS) связана с разбором мультимедиа: аудио/видео, анимированные стикеры, архивы и preview-функции. Автоматический парсинг/рендеринг расширяет риск.
- **Zero-click и цепочки багов — самый опасный сценарий.**
  Уязвимости в низкоуровневых протоколах (VoIP, парсеры форматов) + уязвимости ОС дают эксплойт-цепочки с полной компрометацией без действий пользователя (пример: Pegasus через VoIP).
- **Веб- и десктоп-клиенты.** Web — подвержен XSS/CSRF/краже сессий; Electron-десктопы часто наследуют уязвимости платформы/рендерера.
- **Большая часть CVE происходит из сочетания собственных багов + уязвимостей зависимостей.** Библиотеки (rlottie, media-кодеки, Electron, Skia и пр.) часто являются причиной уязвимостей в клиентах.
- **Разрыв между найденными «багами» и зарегистрированными CVE.**
  Некоторые серьёзные исследования не получают CVE или помечаются как disputed, что осложняет картину и затрудняет агрегированную аналитику.
- **Различия между продуктами.** Популярные централизованные мессенджеры (WhatsApp*, Telegram) имеют больше зарегистрированных CVE просто из-за масштаба и разнообразия пользователей; продукты с меньшей аудиторией/закрытым кодом (Threema) показывают меньше зарегистрированных CVE, но это не обязательно значит «более безопасны».

Базовые рекомендации

- Обновляйте мессенджеры и ОС сразу после выхода security-фиксов
- Отключите автозагрузку медиа/вложений; не открывайте файлы/стикеры от неизвестных отправителей
- По возможности старайтесь следовать принципу наименьших привилегий для приложений
- Регулярно проверяйте и отзывайте linked devices / сессии
- Следите за сведениями об актуальных уязвимостях

Источники

- https://www.cve.org/
- https://nvd.nist.gov/
- Abdur Rahman Onik, Joseph Brown, Clinton Walker, and Ibrahim Baggili. 2025. A Systematic Literature Review of Secure Instant Messaging Applications from a Digital Forensics Perspective. ACM Comput. Surv. 57, 9, Article 239 (September 2025), 36 pages. https://doi.org/10.1145/3727641
- Blerton Abazi and Renata Gegaj. 2022. A comparative study on the user experience on using secure messaging tools. In Proceedings of the Big Data Privacy and Security in Smart Cities. Springer, 119–131.
- Nishchal Soni. 2024. Forensic analysis of WhatsApp: A review of techniques, challenges, and future directions. Journal of Forensic Science Research 8 (2024), 019–024.
- Stiftung Warentest. 2022. Messenger im Vergleich. Retrieved January 19, 2023 from https://www.test.de/Messenger-Apps-im-Vergleich-4884453-0/
- https://habr.com/ru/companies/dcmiran/news/568512/
- https://mtpsym.github.io/paper.pdf
- https://www.ieee-security.org/TC/SP2022/
- https://www.anti-malware.ru/analytics/Technology_Analysis/WhatsApp-Future-in-Russia
- Martin R. Albrecht, Lenka Mareková, Kenneth G. Paterson, and Igors Stepanovs. 2022. Four attacks and a proof for Telegram. In Proceedings of the 43rd IEEE Symposium on Security and Privacy.
- Samantha M. Judge. 2018. Mobile Forensics: Analysis of the Messaging Application Signal. University of Central Oklahoma.
- Kenneth G. Paterson, Matteo Scarlata, and Kien Tuong Truong. 2022. Three lessons from threema: Analysis of a secure messenger. Attack Website (2022).

А уязвим ли мессенджер?

Неуязвимый мессенджер — это как вечный двигатель. Красиво звучит, но в реальности не работает

Благодарю за внимание!