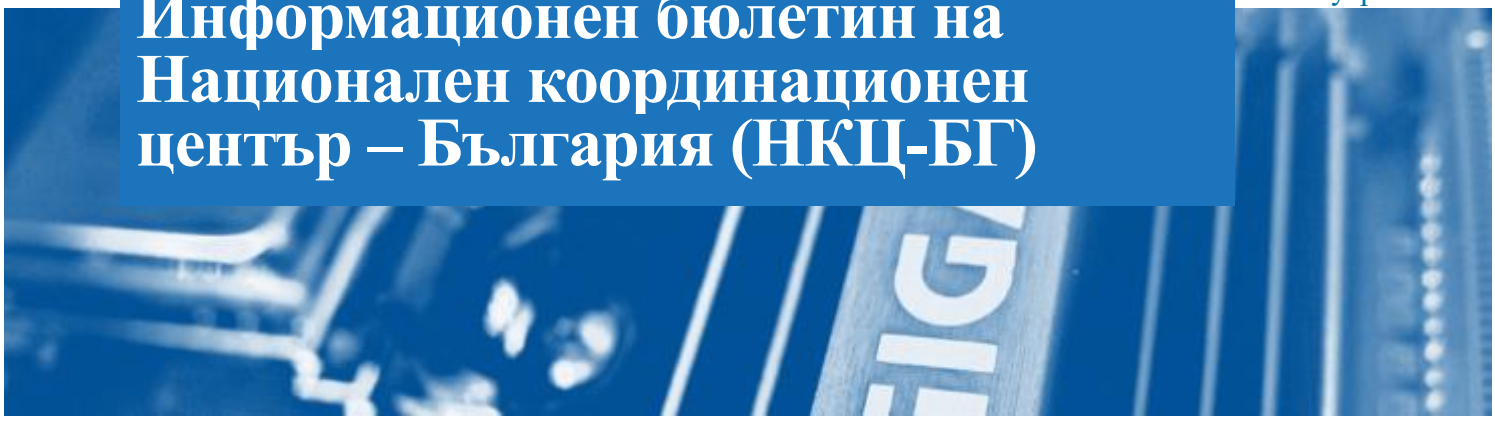
Министерство на електронното управление

Януари 2026

Информационен бюлетин на Национален координационен център – България (НКЦ-БГ)



ОТЧЕТ ЗА 2025 Г. НА ЕВРОПЕЙСКИЯ КОМПЕТЕНТЕН ЦЕНТЪР ЗА КИБЕРСИГУРНОСТ (ECCC)

ЕВРОПЕЙСКИЯ КОМПЕТЕНТЕН ЦЕНТЪР ЗА КИБЕРСИГУРНОСТ (ECCC) публикува отчет за съществените резултати от дейността си за 2025 г.:

✓ Публикувана е първа работна програма по Програма „Цифрова Европа“ за 2025-2027 г., с която са планирани 390 милиона евро инвестиции.

✓ Стартирани са 3 покани за набиране проекти по Програма „Цифрова Европа“ и Програма „Хоризонт Европа“.

✓ Стартирани са обществени поръчки за първата европейска инфраструктура за тестване PQC (post-quantum cryptography).

✓ Продължена е работата по създаването на трансграничните и национални хъбове в съответствие с Законодателен акт в областта на киберсолидарността (Cyber Solidarity Act).

✓ Управление изпълнението на 197 проекта на обща стойност от 604 283 645 евро по поканите за предложения по програмите „Цифрова Европа“ и „Хоризонт Европа“.

ЕВРОПЕЙСКИЯ КОМПЕТЕНТЕН ЦЕНТЪР ЗА КИБЕРСИГУРНОСТ (ECCC) публикува отчет за съществените резултати от дейността си за 2025 г.

Предвижда се фокусът на ECCC за 2026 г. да бъде върху подобряване на портфолиото от проекти за киберсигурност и засилване на киберобщността от заинтересованите страни чрез ATLAS, за да се постигне общата цел „Европа - по-безопасна, устойчива и по-конкурентоспособна дестинация“.



✓ Участие в повече от 160 събития, лично и онлайн, за представяне на Центъра, на неговата работна програма и на отворените покани за набиране на проекти.

✓ Старт на подбора на членове за Стратегическата консултативна група.

✓ Стартира платформата ATLAS за регистрация на киберобщността.

✓ Провеждане на първите съвместни заседания на ECCC-ENISA по време на полското председателство

✓ Разширяване на глобалната мрежа, с подписване на споразумения за сътрудничество с Украйна, Молдова и Европейската агенция за отбрана.

Предвижда се фокусът на ECCC за 2026 г. да бъде върху подобряване на портфолиото от проекти за киберсигурност и засилване на киберобщността от заинтересованите страни чрез ATLAS, за да се постигне общата цел „Европа - по-безопасна, устойчива и по-конкурентоспособна дестинация“.

ПОДКРЕПА ЗА ПО-ДОБРА КИБЕРЗАЩИТА НА МАЛКИЯ И СРЕДЕН БИЗНЕС



ЕВРОПЕЙСКИЯ КОМПЕТЕНТЕН ЦЕНТЪР ЗА КИБЕРСИГУРНОСТ (ECCC) публикува покана за набиране на проектни предложения по програмата „Цифрова Европа“.

Отворената покана CYBER-09-UPTAKE подкрепя разработването и внедряването на инструменти за киберсигурност като услуга, която помага на МСП да управляват киберриска, да инвентаризират активи, да откриват уязвимости и оказват съдействие при възникване на инциденти.

Краен срок за кандидатстване: 31 март 2026 г.



📌 Отворената покана на European Cybersecurity Competence Centre (ECCC) за CYBER-09-UPTAKE, финансирана по програмата „Цифрова Европа“ подкрепя разработването и внедряването на инструменти за киберсигурност като услуга, която помага на МСП да управляват киберриска, да инвентаризират активи, да откриват уязвимости и оказват съдействие при възникване на инциденти.

🎯 Фокус: инвентаризиране на активи, автоматизирана оценка на риска, сигнали за уязвимости и заплахи.

👨‍👨‍👧‍👦 Целева група: МСП и други публични и частни организации, включително от научноизследователската и академичната общност и крайни получатели.

💶 Бюджет: 15 милиона евро

🏛️ БФП: 50%

🗓️ Краен срок: 31 март 2026 г.

🔗 Повече детайли и информация: https://lnkd.in/dTg7pCc4

ДАННИ ЗА М. ДЕКЕМВРИ 2025 Г. ЗА КИБЕРОБСТАНОВКАТА В БЪЛГАРИЯ И ЕС

Анализ на Министерството на електронното показва, че за м. декември 2025 г. в ЕС се запазва тенденцията основната част от киберинцидентите да са от типа DDoS.
В България основно преобладават phishing инцидентите като се отчита лек спад при тях спрямо предходния месец. На второ място са инцидентите от типа Malicious Code (зловреден код) – Trojan. Не са докладвани и регистрирани инциденти от типа Ransomware и типа DDoS.

На годишно ниво може да се каже, че има ръст на Phishing инцидентите спрямо предходните години.
Заради ръста на phishing атаките през последните години е все по-необходимо да се провеждат чести phishing обучения. Те помагат на служителите да разпознават навреме измамните имейли и техники и да реагират правилно. По този начин значително се намалява рискът от пробиви в сигурността, причинени от човешка грешка.



MONGOBLEED — ЕДНА ОТ НАЙ-ГОЛЕМИТЕ УЯЗВИМОСТИ В КИБЕРСИГУРНОСТТА ПРЕЗ 2025 Г.

КАКВО ПРЕДСТАВЛЯВА MONGODB?

• MongoDB е най-употребяваната NoSQL база данни в света. Използва се като градивен елемент на съвременните уеб и облачни приложения. Вместо да съхранява информацията в традиционни таблици с редове и колони като стандартна релационна (SQL) база данни, MongoDB работи с документно-ориентиран модел, при който данните се записват във формат, подобен на JSON (BSON). Това позволява гъвкава структура, лесно разширяване и бързо развитие на приложенията без нужда от строги предварително дефинирани схеми. Платформата е създадена с фокус върху висока производителност, мащабируемост и работа в разпределени среди, което я прави предпочитан избор за нови компанаии, големи технологични компании и критични облачни системи.

MongoDB се използва масово за съхранение на потребителски профили, логове, IoT данни, съдържание в реално време и бекенд инфраструктура на уеб и мобилни приложения. Именно широкото ѝ разпространение и ключовата ѝ роля в модерните технологии превръщат всяка уязвимост в нея — като MongoBleed — в глобален риск за сигурността.

MONGOBLEED

• През декември 2025 г. беше разкрита изключително опасна уязвимост в MongoDB. Уязвимостта получи името MongoBleed и беше проследена под идентификатор CVE-2025-14847 — със сериозност CVSS 8.7, което я поставя сред най-критичните уязвимости на годината.

КАКВО ПРЕДСТАВЛЯВА MONGOBLEED?

• MongoBleed е паметна уязвимост тип memory leak (в буквален превод изтичане на памет) в сървърите на MongoDB, която позволява на неавтентифициран отдалечен нападател да извлече фрагменти от оперативната памет на базата данни, преди проверката за достъп да бъде изпълнена. Това означава, че злонамерените атаки могат да получат достъп до чувствителна информация — пароли, сесийни токени (използвани за логин), ключове за API, конфигурационни данни и други — без да имат потребителско име или парола.



• Причината за уязвимостта е в модула за компресия на мрежовия протокол (zlib) на MongoDB: когато сървърът получава злоумишлено форматирани, компресирани съобщения, логиката за декомпресия неправилно връща памет, която не е инициализирана. Това позволява на нападателя да „изцеди“ (bleed) паметта и да я прочете на части, подобно на по-ранния известен бъг Heartbleed.

ОБХВАТ И ВЛИЯНИЕ

• Уязвимостта беше широко експлоатирана в реалния свят още в края на декември 2025 г. Сканиране на интернет показва, че около 87 000 публично достъпни MongoDB сървъри са били потенциално изложени на риска от атаки, с големи концентрации в САЩ, Китай, Германия и други. Според доклади уязвимостта засяга много поддържани и наследени версии на MongoDB (от версии 3.6 до 8.2), особено ако zlib компресията е активирана — което е често срещана настройка.

РЕАЛНА ЕКСПЛОАТАЦИЯ И ПОСЛЕДСТВИЯ

• Една от най-цитираните истории около MongoBleed е свързана с голяма киберпрестъпна акция срещу компанията Ubisoft, при която хакери успяха да компрометират инфраструктурата на играта Rainbow Six Siege, причинявайки хаос като манипулиране на игрови валути и системи за баниране/разбанване на играчи. Най-вероятно тази атака е успяла да извлече ключови API ключове на играта.

ЗАЩО MONGOBLEED Е ТОЛКОВА ЗНАЧИМ?

MongoBleed се отличава с няколко ключови характеристики:

- Без нужда от автентикация: нападателите могат да експлоатират уязвимостта без каквито и да е валидни идентификационни данни.
- Широко разпространен: уязвимостта засяга десетки хиляди сървъри по света, включително системи от бизнеси и публични услуги.
- Потенциално изтичане на много поверителни данни: фрагменти от паметта могат да съдържат всичко — от идентификационни данни до вътрешни ключове за облачни услуги.
- Рискове за веригата на доставки: компрометирани бази данни могат да послужат като входна точка за по-широки атаки, включително кражба на код, CI/CD токени и други.

КАКВО НАУЧИХМЕ ОТ УЯЗВИМОСТТА НА MONGODB?

• MongoBleed 2025 беше един от най-значимите пробиви в сигурността на бази данни за годината, сравнен по въздействие с исторически уязвимости като Heartbleed. Той напомня за важността на:

- Редовното обновяване на софтуера



- Ограничения достъп до критични системи
- Проактивното управление на риска в инфраструктурите със зависимост от открити бази данни.

• За компаниите и администраторите този инцидент подчерта, че дори „добре конфигурирани“ системи могат да останат уязвими дълго време, ако основните механизми за сигурност не се поддържат актуални.





Министерство на електронното управление

ул. „Ген. Гурко“ № 6

Гр. София 1000

Ел. поща: bnccc@egov.government.bg

Ел. адрес: https://ncc.egov.bg/