

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Изследване на уязвимости и разработка на експлойти

Оригинално изследване на уязвимости и разработка на експлойти срещу софтуер, устройства и протоколи — същата работа, която стои зад публикуваните от нас CVE в уеб приложения и сървърен софтуер, приложена към продуктите, които пускате или използвате.

ПОДХОДЯЩО ЗА	Производители на софтуер и устройства; продукти с високи изисквания; укрепване на защитата преди пускане
ПОЛУЧАВАТЕ	Констатации от изследването, PoC експлойти, подкрепа при координирано разкриване
ОБХВАЩА	Оригинални изследвания и PoC експлойти

Доказано, а не пожелателно

Повечето тестове проверяват за известни проблеми. Изследването открива непознатите — във вашия собствен продукт, в зависимост или в устройство, на което разчитате. Нашият екип прави това на практика, с публикувани CVE в широко използван софтуер.

Разработваме експлойти за доказателство на концепцията, когато са необходими, за да се докаже въздействието, и подпомагаме координираното разкриване, когато изследването засяга трети страни.

Какво изследваме

- Вътрешна логика на уеб приложения и API
- Thick-client и настолен софтуер
- IoT и вградени устройства
- Протоколи и файлови формати
- Зависимости от трети страни
- Разработка на експлойти за доказателство на концепцията

Как протича

- Определяне на целта — Договаряме продукта, дълбочината и подхода към разкриването.
- Изследване — Задълбочен ръчен анализ, обратно инженерство и fuzzing при нужда.
- Доказване — Разработваме PoC, за да демонстрираме реално въздействие.
- Разкриване — Констатации към вас и координирано разкриване, когато е приложимо.

Какво получавате

- Констатации от изследването — Документирани уязвимости с технически детайли.
- Доказателство на концепцията — Работещи PoC, които демонстрират реално въздействие.
- Насоки за отстраняване — Конкретни корекции и съвети за укрепване на защитата.
- Подкрепа при разкриване — Управление на координираното разкриване, когато е необходимо.

Методологии и стандарти, на които се опираме

CVE и координирано разкриване (CVD) · Отговорно разкриване · Оценяване по CVSS · CWE · Методология за fuzzing · Методология за обратно инженерство

Старши тестери. Доказателства за всяка констатация. Включен повторен тест. Минимум пет дни тестване. Обхват и примерни доклади — pxlsec.com/bg/services/vulnerability-research.