



ПРИМЕР ОТ ПРАКТИКАТА

От достъп до един контейнер до целия слой с данни

Финансови услуги · Вътрешен тест за проникване с излизане от контейнер

Доказана верига на компрометиране и спешен план за 24 часа

Анонимизиран съгласно NDA. Клиентът и идентифициращите детайли са премахнати. PXLSecurity LTD. · София, България · pxlsec.com



ПРИМЕР ОТ ПРАКТИКАТА

От достъп до един контейнер до целия слой с данни

Сектор	Финансови услуги
Ангажимент	Вътрешен тест за проникване с излизане от контейнер
Резултат	Доказана верига на компрометиране и спешен план за 24 часа

1	МИЛИОНИ	0
начален достъп до контейнер	достъпни редове от различни клиентски организации	прочетени или извлечени редове с данни

ПРЕДИЗВИКАТЕЛСТВОТО

Доставчик, който обработва регулирани банкови данни за множество банки, искаше да установи какво би могъл да засегне нападател с възможност да изпълнява код в продукционен контейнер на приложението.

КАК СЕ РАЗВИ

1. Започнахме със симулиран достъп до един продукционен контейнер на приложението.
2. Прочетохме дешифрирани тайни, оставени в открит вид при стартирането на контейнера.
3. Установихме, че акаунтът на приложението има права на суперпотребител в достъпния клъстер от бази данни.
4. Чрез метаданни потвърдихме права за четене и запис в десетки бази на клиентски организации, централен набор от данни за кредитен риск и споделеното хранилище за SSO, без да четем клиентски данни.
5. Възстановихме продукционния ключ за подписване на сесии и потвърдихме валидността му офлайн чрез възпроизвеждане на реален подпис. Това позволява подправяне на сесии за всеки потребител, роля или клиентска организация.
6. От същата достъпна конфигурация възстановихме ключ за внедряване чрез GitOps и партньорски ключове за трансфер, съхранявани заедно с паролите си.

ОСНОВНИ КОНСТАТАЦИИ

Critical	Акаунтът на приложението в базата е суперпотребител на клъстера
Critical	Ключът за подписване на сесии може да бъде възстановен от хоста на приложението
High	Дешифрирани тайни, четими в работещия контейнер
High	Изложен ключ за внедряване през GitOps (риск за веригата на доставки)
Medium	Паролите на партньорските ключове се съхраняват заедно със самите ключове

ВЪЗДЕЙСТВИЕ

Достъпът до един контейнер позволяваше достъп до данните на различни клиентски организации, подправяне на сесии за всеки акаунт и компрометиране на механизми за внедряване на софтуера.

РЕЗУЛТАТ

Доказахме цялата верига стъпка по стъпка и предадохме план за най-спешните корекции (P0) в рамките на 24 часа: подмяна на ключа за подписване на сесии, ограничаване на правата на акаунта за базата данни и подмяна на ключовете за внедряване и партньорски трансфер. Обхватът на достъпа беше установен само чрез метаданни — не бяха прочетени редове с клиентски данни.

ТЕХНИКИ

Тайни в работещ контейнер · Прекомерни права в базата данни · Подправяне на сесии · Ключове за внедряване и трансфер · Определяне на обхвата на компрометиране

УСЛУГИ

Тестване за проникване · Тестване за проникване в облачна среда

Работете с PXLSec

Независимо офанзивно тестване на сигурността от 2014 г. — тестване за проникване, red teaming и сигурна разработка, изпълнявани от старши инженери, с доказателство за всяка констатация и повторен тест, който потвърждава поправката.

Заявете предложение: pxlsec.com/bg/contact · hello@pxlsec.com

PXLSecurity LTD. · бул. „Васил Левски“ 12, 1142 София, България · VAT BG203239331