



ПРИМЕР ОТ ПРАКТИКАТА

Публикувано мобилно приложение, което беше трезор за идентификационни данни

Доставчик на корпоративен софтуер · Тест за проникване на мобилно приложение (Android, iOS, Windows)

1 критична, 5 високи — отстранени

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



ПРИМЕР ОТ ПРАКТИКАТА

Публикувано мобилно приложение, което беше трезор за идентификационни данни

Сектор	Доставчик на корпоративен софтуер
Ангажимент	Тест за проникване на мобилно приложение (Android, iOS, Windows)
Резултат	1 критична, 5 високи — отстранени

1C / 5H	3	0
констатации на 3 платформи	тествани операционни системи	извлечени записа

ПРЕДИЗВИКАТЕЛСТВОТО

Доставчик на софтуер поиска проверка на клиентското приложение, което предоставя на други организации, във версиите за Android, iOS и Windows.

КАК СЕ РАЗВИ

1. Разопаковахме приложението и анализирахме съдържанието на пакета и двоичните файлове.
2. Открихме твърдо кодирани сървърни идентификационни данни, компилирани в пакета.
3. Потвърдихме с проверка само за четене, че данните позволяват удостоверен достъп до вътрешен API.
4. Възстановихме ключа за шифроване на локалната база от данни, налични на устройството. Извеждането на ключа не използваше сол.
5. Дешифрирахме локалното хранилище и заобиколихме проверката за jailbreak с едно прихващане на функция по време на изпълнение.
6. Показахме, че настройка по подразбиране в MDM изключва фиксирането на сертификати без предупреждение и позволява прихващане на сесията.

ОСНОВНИ КОНСТАТАЦИИ

Critical	Твърдо кодирани сървърни идентификационни данни в публикувания двоичен файл
High	Ключът за шифроване в покой може да бъде възстановен от устройството
High	Вграден локален сървър разкрива собствения си токен за удостоверяване
High	Настройка по подразбиране в MDM изключва фиксирането на сертификати без предупреждение
Medium	Проверката за jailbreak/root може да се заобиколи с едно прихващане на функция по време на изпълнение

ВЪЗДЕЙСТВИЕ

Нападател с достъп само до публично достъпното приложение можеше да получи достъп до работещ API за данни и да дешифрира локалното хранилище. Пътят беше потвърден и на трите платформи.

РЕЗУЛТАТ

Докладвахме една критична и пет констатации с висока критичност, подкрепени с доказателства. Посочихме кои идентификационни данни трябва да се подменят незабавно и конкретни корекции за извеждането на ключове, фиксирането на сертификати (certificate pinning) и управлението на токени. Прекратихме проверката след доказване на достъпа, без да извличаме записи.

ТЕХНИКИ

Обратно инженерство на двоичния файл · Твърдо кодирани тайни · Слабо извеждане на ключове · Заобикаляне на проверките за jailbreak/root · Заобикаляне на фиксирането на сертификати

УСЛУГИ

Сигурност на мобилни приложения · Тестване за проникване · Сигурна разработка

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