ZIMPERIUM®

How secure are today's mHealth apps?

100
apps tested

741 **vulnerabilities found**

Top 3 threats

Every Android app and 72% of iOS apps had four or more security flaws

iOS

1. ZipperDown vunerability leading to remote code execution attacks
2. Sensitive data in NSUserDefaults
3. Sensitive information in property lists

Android

1. Unused permissions
2. Disabled SSL CA validation and certificate pinning
3. ByteCode obfuscation missing

Key findings

Major security gaps revealed in mobile medical apps

71% of apps have at least one **high-level vulnerability**

85% of COVID tracking apps **leak data**

91% of apps **fail critical cryptographic tests**

34% of **Android** apps are vulnerable to **encryption key extraction**

28% of **iOS** apps are vulnerable to **encryption key extraction**

83% **of high-level threats could have been mitigated using in-app protection**

Protect your mobile apps, healthcare data, doctors, and patients

Data breaches cost healthcare providers an average of $9.23 million per breach. Yet, our assessment indicates the healthcare industry has failed to scale up its security practices.

Download the full report now