MEDTECH INSIGHT
CITELINE COMMERCIAL

30 Aug 2022 | **News**

Mobile Health Apps Are Falling Behind In Cybersecurity, Report Finds

by Hannah Daniel

A report commissioned by Approov found that mobile healthcare apps are falling behind their counterparts in technology.

A study of 30 mobile healthcare (mHealth) apps discovered that every app studied was vulnerable to cybersecurity attacks.

Osterman Research found that the demand for mobile apps tripled between 2020 and 2022 due to the pandemic and the need for virtual options, and mHealth apps were no exception. There were 318,000 mHealth apps on the market in 2018, with over 3.7bn downloads, the report stated. A separate April 2020 report by Reports and Data predicts that the global mHealth market will reach $312bn by 2027.

Financial and healthcare industries have fallen behind technology industries in terms of security the researchers found. Osterman found that healthcare and finance industries had two to three times less *visibility* on the occurrence of cybersecurity incidents, meaning that organizations don't have the tools to monitor cybersecurity threats and breaches.

43% of the Osterman survey respondents in the healthcare industry said that their business or organization prioritized new features over keeping on top of security.

There has also been an increase in cyber attacks on healthcare organizations and hospitals in recent years, research by Cynerio and Ponemon Institute found. Of 517 healthcare systems surveyed in the US, almost half reported being hit with ransomware, with 75% of them being hit more than once. (Also see "*As Cyberattacks On Hospitals Rise, Medical Devices Are Particularly Vulnerable*" - Medtech Insight, 16 Aug, 2022.)

The Food and Drug Administration is aware of the issues and published a draft guidance on 8 April to update cybersecurity recommendations for medical devices. (Also see "*FDA's Schwartz*

Says New Draft Cybersecurity Guidance Addresses Emerging Threats" - Medtech Insight, 12 Apr, 2022.)

API Vulnerabilities Allow Access To Personally Identifiable information

Selling medical records is a lucrative business on the black market. While a social security number will sell for $1 and credit cards for around $100, medical records can sell for up to $1,000, researcher Alissa Knight at Knight Ink explains in a report issued in July.

The report was commissioned by Approov, a mobile app protection specialist, and titled "*All That We Let In: Hacking 30 Mobile Health Apps and APIs.*"

Application programming interfaces (APIs) communicate with applications and databases to pass information back and forth.

After hacking 30 different mHealth apps, Knight was able to compromise them all and access patient records and personally identifiable information.

Knight reported that 50% of the app's APIs were able to be exploited to allow access to pathology reports, x-rays, and medical results of patients that Knight shouldn't have had access to.

Additionally, half of the APIs allowed Knight to see patient hospital admission information that she should not have had access to.

All of the APIs tested were vulnerable to Broken Object Level Authorization Attacks (BOLA), allowing Knight to switch out object data within the code that granted access to different accounts and records. These BOLA vulnerabilities were found in under one minute in each mHealth app.

Hardcoding credentials into application software can also lead to vulnerabilities, and sensitive information such as passwords and credentials can be easily found within the application software if a hacker knows where to look. Knight reported that 77% of the mHealth apps contained hardcoded API keys, tokens, and credentials, and 7% contained hardcoded keys to third party payment processors.

mHealth Apps Are Responsible for Keeping Data Safe

Healthcare companies have a responsibility to protect their data, Knight concludes, especially considering the vulnerabilities found in mHealth *apps.*

"If you've never been convinced because of a lack of empirical evidence, that security needed to shift-left in your organization, here is your proof," Knight tells mHealth companies.

There was also recent social pressure on period tracking apps to safeguard their consumer's data after the overturning of Roe v. Wade and the possibility of criminalizing people who get abortions. (Also see "*Period-Tracking Apps Should Safeguard Data, Reassure Customers In Post-Roe Era*" - Medtech Insight, 1 Jul, 2022.)