HBW INSIGHT
CITELINE COMMERCIAL

06 Sep 2022 | **News**

Weak Cybersecurity In Mobile Health Apps Puts Users' Medical Records At Risk, Reports Find

by Hannah Daniel

Osterman Research says health care sector is behind technology industries in cyber-protecting mobile and other apps. Separately, consultant Knight Ink hacked 30 mobile health apps, compromised all of them and accessed patient records and personally identifiable information.

Every mobile health care app studied by Osterman Research Inc. was vulnerable to cybersecurity attacks, while Knight Ink LLC's research showed apps in the category could be compromised to allow access to patient records and other restricted information.

Osterman Research found that demand for mobile apps tripled between 2020 and 2022 due to the COVID-19 pandemic and consumers' growing demand for virtual options. The mobile health care (mHealth) piece of the market was estimated in a 2020 report by Reports and Data predicts to will reach $312bn globally by 2027.

Among Osterman's survey respondents in the health care industry, 43% said their business or organization prioritized new features over keeping on top of security.

Osterman, with its US office in Black Diamond, WA, says in addition to the health care sector, financial industries have fallen behind technology industries in terms of security its researchers found. It found that health care and finance industries had two to three times less visibility for cybersecurity incidents, meaning those organizations don’t have the tools to monitor cybersecurity threats and breaches.

Cyber attacks on health care organizations and hospitals have increased 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, 75% 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The Food and Drug Administration is aware of the issues and published a draft guidance in April to update cybersecurity recommendations for medical devices.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.)

Additionally, social pressure has increased recently on menstrual cycle tracking apps to safeguard users' data after the US Supreme Court's ruling in Dobbs v. Jackson (Mississippi) Women's Health Group allowed states to restrict or ban access to abortion services. (Also see "*Period-Tracking Apps Should Safeguard Data, Reassure Customers In Post-Roe Era*" - Medtech Insight, 1 Jul, 2022.)

API Vulnerabilities Allow Access To Personal 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, Las Vegas-based online content and cybersecurity consultant Knight Ink explained in a report published in July, "*All That We Let In: Hacking 30 Mobile Health Apps and APIs*," commissioned by Approov, a mobile app protection technology and services provider owned by CriticalBlue Ltd., of San Jose, CA.

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

After hacking 30 mHealth apps, Knight Ink partner Alissa Knight reported she compromised all of them and accessed patient records and personally identifiable information. She said 50% of the app's APIs could be exploited to allow access to pathology reports, x-rays and other restricted medical records.

Additionally, half of the APIs also allowed Knight to see patient hospital admission information.

All of the APIs tested were vulnerable to broken object level authorization attacks (BOLAs), allowing Knight to switch out object data within the code that granted access to different accounts and records. The BOLA vulnerabilities were found in under one minute in each mHealth app.

Hard-coding 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 77% of the mHealth apps contained

hardcoded API keys, tokens, and credentials, and 7% contained hardcoded keys to third party payment processors.

Health care companies have a responsibility to protect their data, Knight concluded, especially considering vulnerabilities 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,” she advises.

This article is an update on reporting initially published by Citeline's Medtech Insight newsletter.