approov

API THREAT PROTECTION

www.approov.io

“Knight Ink Research Report: Playing with FHIR: Hacking and Securing FHIR APIs” - Summary of Findings

The report was published on October 13th 2021 and is available here: https://approov.io/for/playing-with-fhir/

Introduction

In research sponsored by Approov, Alissa Knight of Knight Ink spent the last year focusing on hacking Fast Healthcare Interoperability and Resources (FHIR) APIs, working with some of the world's largest Electronic Health Record (EHR) providers in her vulnerability research. This report, covering all enterprise types in the FHIR ecosystem, represents her findings, and underscores a systemic lack of basic protections in parts of the ecosystem - enabling unauthorized access to an inordinate amount of patient records.

Quotes from the Report

“An effective kill chain in the targeting of the healthcare industry will not be of the EHR systems running in the providers, but in the third-party FHIR aggregators and third-party apps which access these EHR APIs as data moves from higher security levels to third-party aggregators where security has been found to be flagrantly lacking.”

“The findings in this report will show that of the 5 FHIR APIs I tested (two of which were EHR vendors with no vulnerabilities) - an ecosystem of 48 FHIR apps with aggregated EHR data from over 25,000 healthcare providers and payers - contained pervasive server-side authentication and authorization vulnerabilities that allowed me to access over 4 million patient and clinician records with my own patient login. "

Alissa Knight

approov

Executive Summary

- **New opportunities, new players, high growth**: Fast Healthcare Interoperability and Resources (FHIR) is the data exchange API specification at the heart of this ecosystem mandated by the ONC to enforce patient control of healthcare data - creating a dynamic and evolving ecosystem of new and existing players. According to Zion Market Research, the mHealth apps market is anticipated to have a CAGR of 38% until 2025 when it will be worth USD 111.1 billion.

- **Healthcare data is priceless**: Protected health information (PHI) is worth much more on the dark web than a U.S. credit card, and impossible to "cancel" when lost.

- **The problem is when the data leaves the building**: When data leaves the clinical system, HIPAA no-longer applies. Outside of the EHR systems, app developers and aggregators join the ecosystem, and responsibility for data privacy becomes ambiguous - which is why the FTC made clear on Sept 15 2021 that the Health Breach Notification Rule applies to **any entity** handling healthcare data. Based on the research performed in this study, the security of the EHR platforms was found to be good. However, as testing branched outwards from the EHR providers to third-party clinical data aggregators and mobile apps, vulnerabilities were widely systemic allowing access to EHR data.

- **FHIR is secure but the “last mile” to the apps is not**: Vulnerabilities discovered in this research are not inherent to FHIR, which is a “blueprint” or framework. How it is implemented is up to the developer. Hackers are efficient and will always locate and exploit the weakest link in the chain which, based on this report, is in the healthcare data aggregators and mobile apps which rely on EHR data to deliver their services.

- **Shift left but shield right**: There is an urgent need to apply API security shielding solutions to prevent the exploitation of weaknesses in the mobile healthcare app ecosystem by scripts and automated tools. Such shielding will immediately protect sensitive personal data from exfiltration while the underlying vulnerabilities are addressed.

approov

Key Findings

- Five production FHIR APIs serving an ecosystem of 48 apps and APIs were tested (2 were from EHR vendors and did not show vulnerabilities)
- The ecosystem covered aggregated EHR data from 25,000 providers and payers
- 4m patient and clinician records could be accessed from 1 single patient login account
- 53% of mobile apps tested had hardcoded API keys and tokens which could be used to attack EHR APIs
- 100% of FHIR APIs tested allowed API access to other patient's health data using one patient's credentials.
- 50% of clinical data aggregators did not implement database segmentation allowing access to patient records belonging to other apps developed on their platform for other providers.
- 100 percent of the mobile apps tested did not prevent person-in-the-middle attacks, enabling hackers to harvest credentials and steal or manipulate confidential patient data.

approov

Recommendations to the Regulator*

- Ensure the Information Blocking Rules allow service-providers and EHR vendors to assess the security of the apps and APIs of the aggregators and application developers who connect to their APIs through regular penetration testing and a review of their security controls.
- Clarify that the Security Exception to the Information Blocking Rule allows EHR vendors to require specific controls be implemented by any system that connects to their APIs.
- Reinforce the security guidelines, specifically with requirements around tokens and scopes (which are currently recommendations) to ensure that all organizations who transmit, process, and store EHR data are properly securing their implementation of FHIR.
- Mandate that certificate pinning should be implemented on all SMART on FHIR mobile apps.
- Mandate that shielding solutions must be deployed to ensure that only legitimate applications and users can communicate with APIs to prevent EHR data leakage via synthetic traffic generated by tools, scripts and bots.

* U.S.Department of Health & Human Services (HHS), as mandated by Congress,

approov

Recommendations to FHIR API Owners

- Overall, you must put in place a plan to protect data even when it has left your system. Put in place a process to assess the configuration and implementation security of any third-party apps before allowing access to your EHR and understand the security controls they have in place.
- Employ an API threat management solution that prevents data from leaving via your API endpoints unless the incoming request is tokenized. This will eliminate a lot of the bandwidth wasted to synthetic traffic generated malicious scripts, bots and automated tools. Put in place app and device attestation checks at your API endpoints and require any apps connecting to your endpoint to implement this control.
- Penetration testing performed by a penetration tester with specific skills in testing APIs should be performed. More than 60% of the apps and APIs which were tested contained vulnerabilities allowing unauthorized access to data outside of of authorized user scope. The vulnerabilities seem to be in the apps being created for these EHR systems, not the EHR systems themselves. Penetration testing should include fuzzing APIs as a final step in your penetration testing efforts of an API.
- Inventory your APIs. You can’t protect what you don’t know you have. Ensure you know how many APIs you have, ensure they are all part of your enterprise vulnerability and patch management strategy, and know whether or not they are transmitting, processing, and storing sensitive or regulated data, such as PII, PCI, or PHI.

Recommendations for App Developers

- Obfuscation of mobile app code to secure source code against decompilers isn't enough. Run-time shielding is also needed to prevent tampering with the mobile app or its environment. You must authenticate the app and device using SDK-powered solutions that attach a token to the API request. By using solutions that allow you to compile your mobile app with their SDK, you eliminate developer friction and limit the disruption to your existing software development lifecycle (SDLC) while gaining increased privacy of any secrets hardcoded in the app.
- Put in place a solution for app, user and device attestation to ensure that only genuine apps running in secure environments can access the APIs, thereby eliminating any bots masquerading as your app.
- Implement certificate pinning between app and API to eliminate WitM attacks. Tools are available to make this easy to deploy and administer.
- Third-party app developers and aggregators need to shift their security left and shield right when they deploy. None of the APIs tested seemed to be behind API threat management solutions.
- If you aggregate data, don't use the same database to store the patient records for each provider. This creates the potential for all of your EHR data to be leaked as a result of a vulnerability in just one of the apps. Each microservice should have its own isolated database.

approov

Conclusion

Interoperability rulings by the U.S. Department of Health & Human Services (HHS) are designed to give patients access to information that resides inside their electronic health records (EHR).

During the period leading up to the release of these rulings, EHR vendors and healthcare leaders expressed the concern that patient data from electronic medical records could be compromised by consumer apps, which don't necessarily afford the same protections patients have come to expect from HIPAA.

This research proves that these fears were well founded. However, solutions exist and should urgently be deployed by the healthcare community to better protect patient data all the way to the consumer.

approov

Approov Solution

- Approov provides a patented cloud-based run-time shielding solution which is easy to deploy and protects your APIs and the channel between your mobile apps and APIs from any automated attack.
- By ensuring only an untampered genuine mobile app running in an uncompromised environment can access the API, Approov prevents the exploitation at scale of:
    - Stolen user identity credentials via bots.
    - Vulnerabilities in your apps or APIs, irrespective of whether the vulnerabilities are already known, uncovered through testing or “zero-day”.
    - Malicious business logic manipulation of the API
    - Man in the middle attacks.
- Integration involves including an SDK in your mobile app and adding an Approov token check in your backend
- A full set of frontend and backend Quickstarts are available to facilitate integration with common native and cross-platform development environments.
- A full range of integrations are available eg with API Gateways, WAF, browser fingerprinting etc.

approov

Approov Offer for FHIR API Providers

Approov FHIR Guard puts in place controls in the API endpoint to be able to protect the API and stop the threats described in the report. App owners who choose to integrate Approov will pay per use for the service. Approov prevents bots, scripts and compromised apps from:

- using stolen user identity credentials
- exploiting vulnerabilities in APIs
- malicious manipulation of the business logic of the APIs
- executing Man-in-the-Middle attacks
- complimentary API security solution for “last mile” security

Approov offers the solution and deployment assistance of the end-point protection element free of charge to FHIR API providers who deploy production FHIR APIs handling real patient data. This makes it easy for 3rd parties downstream of the APIs to deploy Approov and augment the security of their apps by putting in place app and client attestation to better protect the channel to the end-user.

Email FHIRGuard@approov.io to confirm that your organization qualifies for this offer.

approov

Quote from the Sponsors

“We see it as a positive step that open APIs are already creating a plethora of healthcare services which are being adopted and appreciated by patients and consumers. However, healthcare organizations and regulators who handle and oversee this sensitive data must give equal attention to security enforcement as they do to empowering citizens to take control of their patient data. With this research we don’t just want to raise yet another red flag about security. The introduction of FHIRGuard is a genuine effort by Approov to contribute positively towards improving the situation today, ahead of regulations which will surely follow.”

David Stewart, CEO, Approov