Health Sector Cybersecurity Coordination Center (HC3)
Analyst Note
April 26, 2021 TLP: White Report: 202104261500

Application Programming Interfaces and Healthcare Cybersecurity

Executive Summary

Application Programming Interfaces (APIs) are a critical component to modern health information technology infrastructures. Due to their role in passing information between resources, they present themselves as an enticing target for attackers to either carry out data breaches or as hop points for further compromise. Understanding how they fit into a healthcare enterprise environment along with the associated security concerns they carry with them is a necessary but not sufficient part of protecting against common threats to healthcare in cyberspace. They are common targets among many threat actors and due to their versatility, they are frequently targeted regardless of the specific goal of the attackers.

Background – What are APIs and how do they fit into an Enterprise Infrastructure?

Application Programming Interfaces are relatively small software components that serve as a seamless interface allowing two applications or resources to talk to each other. In modern implementations, they are often the intermediary process engine that sits between a user-facing application and a database, cloud, or other resource which provides information or a service. From a developer's perspective, the API enables separate software platforms to be continuously developed without interruption in their interoperability. APIs are one example of an iterative development methodology which, along with others such as DevOps, DevSecOps and Agile, enable incremental upgrades of application components to be quickly deployed to consumers without having to first submit to the longer quality assurance lifecycles of legacy technologies. APIs allow software applications to work well together even as they are upgraded over time.

APIs and their Frequent use in Healthcare

Research from 2018 shows healthcare consumers increasingly using digital technology, specifically the use of mobile applications (called "mHealth apps" when developed for healthcare), electronic health records and wearable technologies, with almost half of all healthcare consumers using mHealth apps, compared to just 16% in 2014.[i] Mobile health applications are common, as one 2017 study found that there were no less than 84,000 mobile health application developers and 325,000 mobile health apps available on the market, with growth of more than 30% in both the number of developers and apps as compared to 2016.[ii] These technologies involve the transfer and accumulation of very large quantities of healthcare data, but this data is often stored in multiple forms across many different systems, making it siloed and therefore difficult to access. APIs serve to address this fragmentation, which is true of many types of healthcare data including patient data, electronic health records (EHRs) and wearable biometrics as well as public health information such as surveys, statistics, and recommendations and even clinical trial data. APIs are especially applicable to the healthcare industry and public health. They serve to make healthcare data seamlessly accessible to those authorized, but when compromised, they offer an attacker a unique path to large sets of data that can prove valuable.

API Security and Recommendations

APIs present a valuable target in healthcare organizations because of what they utilize and protect: health data. Healthcare information is highly monetizable by cybercriminals. Stolen health credentials are known to be worth 10 to 20 times the value of credit card numbers and the entire healthcare industry is estimated to be worth about $3 trillion.[iii] Medical records are exceptionally valuable with some studies indicating that they can be sold on the black market for as much as $1,000 each.[iv] Furthermore, APIs are ubiquitous in the healthcare industry and, combined with the valuable data, they have therefore become a potential gateway for malicious activities, especially those allowing cybercriminals to commit fraud. Many of the threats to APIs are the same for other technologies in terms of threat actors as well as tactics, techniques and procedures (TTPs). Many actors who attack healthcare organizations will simply attack unprotected APIs as another vector to achieve their ultimate goal for the attack. There are basic principles regarding the implementation of APIs that should be considered when developing a healthcare application. As such, healthcare organizations should favor applications utilizing APIs that abide by these basic principles:

1. API Management: API management is the full-lifecycle process of designing, deploying, controlling, analyzing and documenting APIs that connect applications and data across enterprise networks and clouds. API management seeks to enable an organization to guarantee functionality and security of both public and internal APIs. This includes monitoring activity for utilization against requirements as well as detection of anomalous activity. API management is critical as it facilitates greater understanding and control of APIs and allows for the use of APIs to monitor activity and usage. As healthcare becomes further digitized and services such as telehealth and telemedicine continue to expand, authorization and authentication should increasingly occur at the front end of the architecture. API management functionality offers traffic monitoring to flag unexpected activity such as out-of-sequence or expired API requests as well as automated enforcement of enterprise security policies. Finally, management also includes maintaining an inventory of all APIs which should be subject to periodic updating.

2. Understanding API functionality: To secure APIs, security professionals must first understand the particular API's functionality and purpose and how it aligns with that organization's operational/business goals. This information should come from the manufacturer or the in-house development team but can get lost in cross-functional communication. Documentation, when properly conducted, can improve this process significantly.

3. Authentication/Authorization: Lack of proper authentication/authorization functionality in an API can create an easily-exploitable opportunity for compromise and leakage of important data such as credentials, personally identifiable information (PII) or personal health information (PHI). APIs often provide an entry point into an organization's databases, and therefore it's important to control access to them. When practical, solutions based on reputable, proven authentication and authorization mechanisms such as OAuth2.0 and OpenID Connect are recommended.

4. Encryption: Encryption of traffic is also critical, and the Transport Layer Security (TLS) protocol is recommended for organizations whose APIs routinely exchange sensitive data (such as login credentials, PII, PHI, credit card, social security, banking information, etc.) TLS encryption should be considered standard and essential, and can be implemented as one-way TLS, or the more recommended implementation, two-way TLS. The most recent version of TLS should always be used, which is 1.3 as of the release of this document.

5. Minimizing Information Leakage: Because APIs frequently contain information that should not be shared such as passwords and cryptographic keys, special attention should be made to ensure this information is continuously protected and not exposed to anyone or anything that lacks proper authorization. It's critically important information leakage is considered when APIs are initially designed as well as during any update development.

6. Input Validation: Information should never be passed from an API without first being validated against each of the data fields' requirements. Input validation is the examination of data as it is received to ensure it conforms to the expected format and is not malformed in any way which could trigger a system malfunction or prompt any other undesirable effect such as system compromise or information leakage. Input validation should happen as early as possible in the data flow, ideally as soon as the data is received from the transmitting source or party. Information from all untrusted sources should be subject to input validation, including that from suppliers, partners and vendors. While input validation can prevent certain cyberattacks such as buffer overflows, denial of service attacks, cross-site scripting attacks and SQL Injections, it should not be used as the primary method of defense against these forms of malicious activity.

7. Service API Implementation: Service APIs are a model of API implementation which involves the functionality of the resources themselves (website, application, service, etc…) to be consolidated in the API, standardizing it across the enterprise. This allows for many resources to reuse a set of common functionalities implemented only once, leveraged by many applications, websites and other services. There are a number of benefits to utilizing service APIs: Consistent implementation of common functionality across applications, reduction of maintenance costs, efficient integration of third party applications as well as robust and improved security. It's worth noting that Service APIs can bring with them additional security issues if not properly implemented. For example, as on-prem services move into the cloud, these software-as-a-service offerings allow connection via HTTP/web browsers. Many of these services are only available via service APIs, which creates security challenges based on the sheer volume of data and the variations of security/authentication models, often across multiple organizations. Due to the lack of inherent trust between different organizations, security and authentication models should be developed along with Service APIs.

8. Principle of Least Privilege – Security should not be an afterthought but an initial priority when implementing APIs. As a foundational security concept, the principle of least privilege should always be practiced, especially when designing and deploying APIs. Access to information or resources should only be limited to those who need it, and only just enough to satisfy their requirements. Limitations based on role, time, status, among other criteria, can and should be implemented as much as possible, in order to balance access with security.

Example API Compromise: SolarWinds

The supply chain attack on the Solar Winds platform, Orion, discovered in December 2020, is known to have compromised nine US federal agencies and at least 100 private sector companies. However, there were believed to be multiple attacks originating from multiple state-sponsored threat actors from several different countries on Orion, with one of them using the malware dubbed Supernova. While Sunburst modified the Orion software on SolarWinds' infrastructure prior to customer download and installation, Supernova modified the Orion code on each individual customer's infrastructure. Supernova contained two components: an unsigned .dll file crafted to appear as legitimate Orion code which was in actuality a web shell, and an exploit that targeted an API authentication bypass flaw (CVE-2020-10148) which was used to run the web shell. Successful exploitation meant an attacker could execute commands without authenticating to the API, which the attackers then used to install the web shell and then leverage follow-up techniques to continue to further stages of the attack. Healthcare organizations using SolarWinds software were impacted by the compromise. This is one example of how an API can be exploited by a cyberattacker to grant them open access to a victim network.

References

Trends in EMR Interoperability
https://chimecentral.org/wp-content/uploads/2021/01/Trends-in-EMR-Interoperability_CHIME_KLAS.pdf

Health Data APIs: Accessing Patient Records, Medical Surveys, and Clinical Studies
https://www.altexsoft.com/blog/health-data-apis/

What you need to know about healthcare APIs and interoperability
https://www.healthcareitnews.com/news/what-you-need-know-about-healthcare-apis-and-interoperability

The Rise of mHealth Apps: A Market Snapshot
https://liquid-state.com/mhealth-apps-market-snapshot/

Health Data APIs: Accessing Patient Records, Medical Surveys, and Clinical Studies
https://www.altexsoft.com/blog/health-data-apis/

84,000 health app publishers in 2017 – Newcomers differ in their go-to-market approach
https://research2guidance.com/84000-health-app-publishers-in-2017/

Your medical record is worth more to hackers than your credit card
https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

Here's How Much Your Personal Information Is Selling for on the Dark Web
https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

What is API management?
https://www.redhat.com/en/topics/api/what-is-api-management

Securing APIs: 10 Best Practices for Keeping Your Data and Infrastructure Safe
https://www.f5.com/labs/articles/education/securing-apis--10-best-practices-for-keeping-your-data-and-infra

Healthcare Cyberthreats: An API-First Approach To Protection
https://www.forbes.com/sites/forbestechcouncil/2021/12/28/healthcare-cyberthreats-an-api-first-approach-to-protection/?sh=6d03cece777e

Health Data APIs: Accessing Patient Records, Medical Surveys, and Clinical Studies
https://www.altexsoft.com/blog/health-data-apis/

100% of Tested mHealth Apps Vulnerable to API Attacks
https://www.hipaajournal.com/100-of-tested-mhealth-apps-vulnerable-to-api-attacks/

Emerging Role of Open APIs in Healthcare: 5 Trends to Know
https://hitconsultant.net/2017/01/13/37163/#.YHcHYSWSmUk

How Can APIs Bring Digital Healthcare Transformation?
https://mobisoftinfotech.com/resources/blog/how-can-apis-bring-digital-healthcare-transformation/

Mobile Health Apps Are Exposing PII and PHI via API Vulnerabilities; 23 Million May Be Affected
https://www.cpomagazine.com/cyber-security/mobile-health-apps-are-exposing-pii-and-phi-via-api-vulnerabilities-23-million-may-be-affected/

API Security Outlook: A Guide to API Security in a Digitally Transformed World
https://cisomag.eccouncil.org/api-security-outlook-a-guide-to-api-security-in-a-digitally-transformed-world/

OWASP API Security Project
https://owasp.org/www-project-api-security/

CVE-2020-10148
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10148

SolarWinds Orion API authentication bypass allows remote command execution
https://kb.cert.org/vuls/id/843464

Automation, zero-trust, API-based security priorities for EMEA CISOs
https://www.computerweekly.com/news/252499676/Automation-zero-trust-API-based-security-priorities-for-EMEA-CISOs

What We Know (and Don't Know) So Far About the 'Supernova' SolarWinds Attack
https://www.darkreading.com/attacks-breaches/what-we-know-(and-dont-know)-so-far-about-the-supernova-solarwinds-attack-/d/d-id/1340513

An Introduction to Service APIs
https://inviqa.com/blog/introduction-to-service-apis

Understanding cyber threats to APIs
https://www.helpnetsecurity.com/2020/06/05/api-security-threats/

Make sure you keep an eye on your APIs
https://www.helpnetsecurity.com/2019/08/13/improving-api-security/

5 Security Challenges to API Protection
https://www.darkreading.com/5-security-challenges-to-api-protection/a/d-id/1334475

Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem
https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem

What you need to know about the new OWASP API Security Top 10 list
https://www.csoonline.com/article/3452747/what-you-need-to-know-about-the-new-owasp-api-security-top-10-list.html

State-sponsored actors may have abused Twitter API to de-anonymize users
https://www.helpnetsecurity.com/2020/02/04/de-anonymize-twitter-users/

Three Factors To Consider In Your Web Application And API Cybersecurity Solution
https://www.forbes.com/sites/forbestechcouncil/2020/04/07/three-factors-to-consider-in-your-web-application-and-api-cybersecurity-solution/?sh=6c056f685e59

The Growing Importance of API Security
https://www.cyberdefensemagazine.com/the-growing-importance-of-api-security/

Week in review: API security risks, Office 365 security pain points
https://www.helpnetsecurity.com/2020/02/23/week-in-review-api-security-risks-office-365-security-pain-points/

Endnotes

[i] https://liquid-state.com/mhealth-apps-market-snapshot/
[ii] https://research2guidance.com/84000-health-app-publishers-in-2017/
[iii] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
[iv] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/