LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

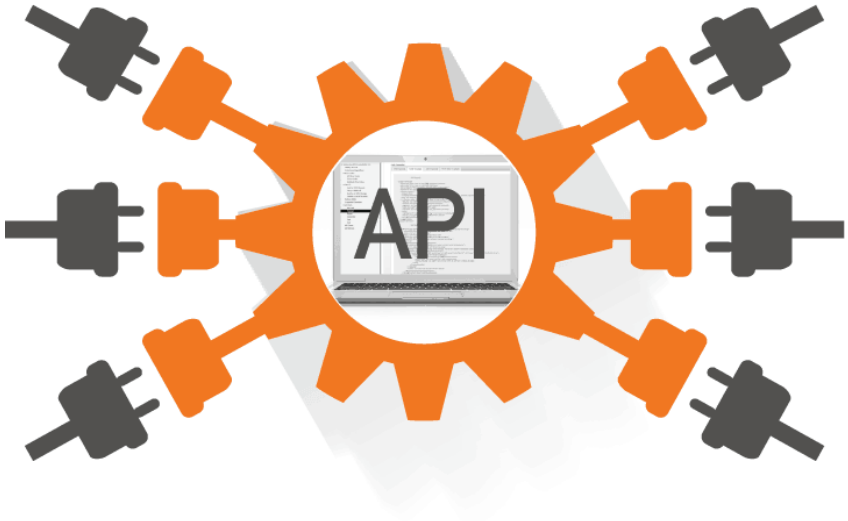
API Security for Healthcare

05/20/2021

TLP: WHITE, ID# ***202105201300***

Agenda

- What are APIs?
- What Are API Components?
- APIs in Use
- What's Driving Their Use, Especially in Healthcare?
- APIs and Healthcare: Why are APIs Attractive Attack Vectors?
- API Protocols
- APIs: The Value to the Healthcare Enterprise and Healthcare Consumers
- Examples of Healthcare APIs
- API Security Recommendations



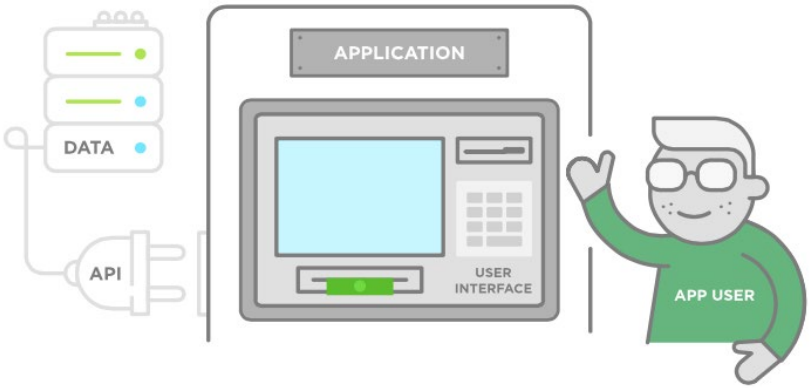
Slides Key:

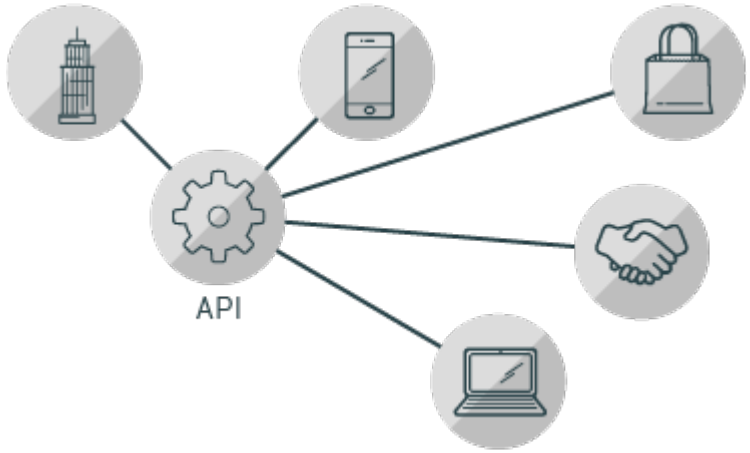
Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What are APIs?

- **A**pplication **P**rogramming **I**nterface:
  - Application – Software that serves a specific purpose
  - Programming – The designing of an application; also known as coding
  - Interface – To come between two entities or organizations for the purposes of exchanging information
- Relatively small software components that serve as a seamless interface, allowing two applications or resources to talk to each other
- Intermediary process engine that sits between a user-facing application and a database, cloud, or other resource, which provides information or a service
- Facilitates modularity in software/application development, enabling separate software platforms to be continuously developed without interruption in their interoperability
- Bottom line: An API facilitates seamless data transfers



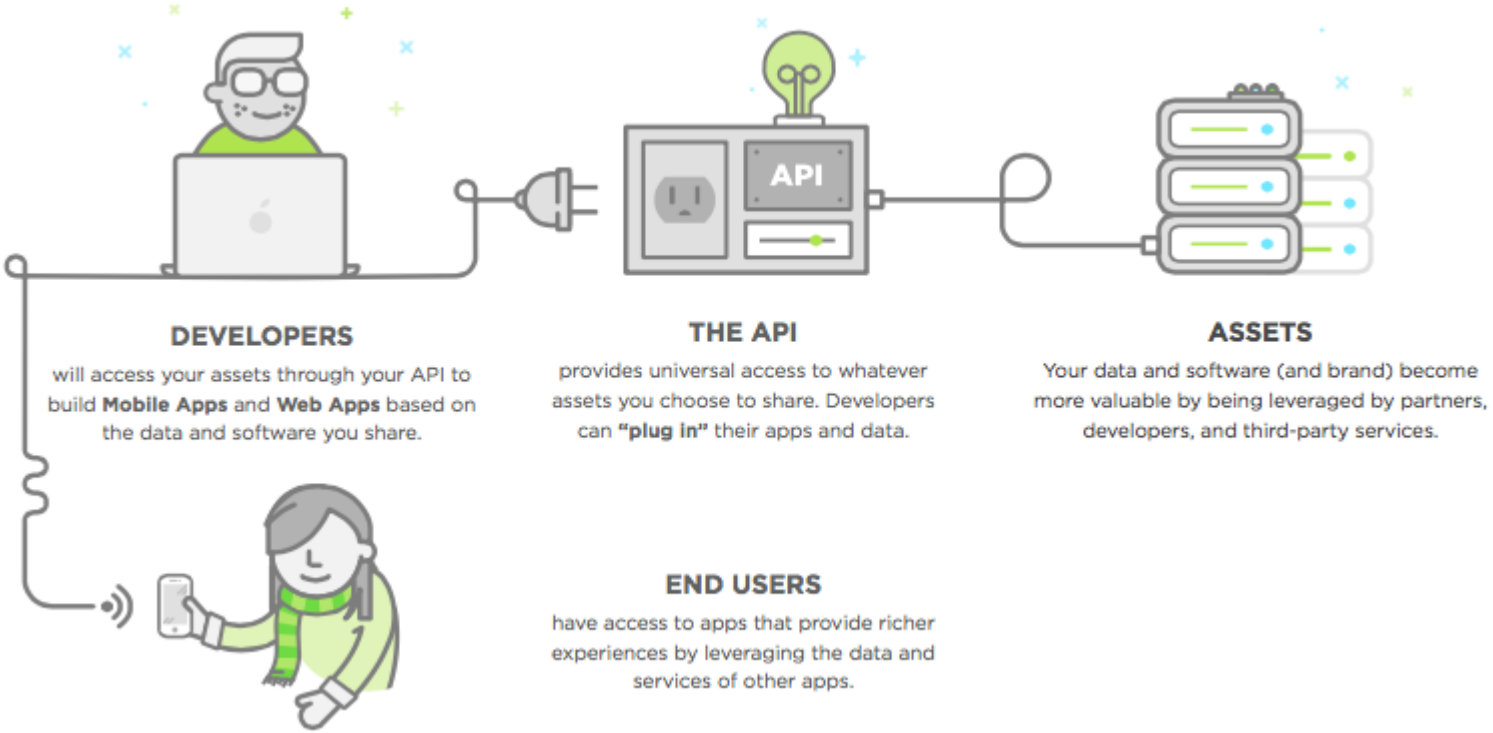


What are the components of an API ecosystem?

- **Assets** – This is the information that is to be shared internally and/or externally with end users. This can be anything from software code to raw or enriched data to full-fledged services
- **APIs** – The APIs themselves; The gateway/filter to separate the assets from the end users who need access to them
- **Developers** – The developers are those who develop the applications that communicate via APIs. This audience is the most direct audience for the APIs.
- **Software/Applications** – These are the applications which provide the services for the end users
- **End Users** – These are those who are requesting access to assets and/or software/applications and are being granted that access via the use of APIs

How do all these components work together?

- “End users” access the apps
- These apps are created and maintained by developers who work with APIs
- The APIs allow for the end users, via an app, to access assets for data and/or services
- Interoperability!



APIs: What's Driving Their Use, Especially in Healthcare?

Why are APIs becoming so common? The technologies that utilize them are ubiquitous.

Especially important is the increasing availability and popularity of mHealth apps

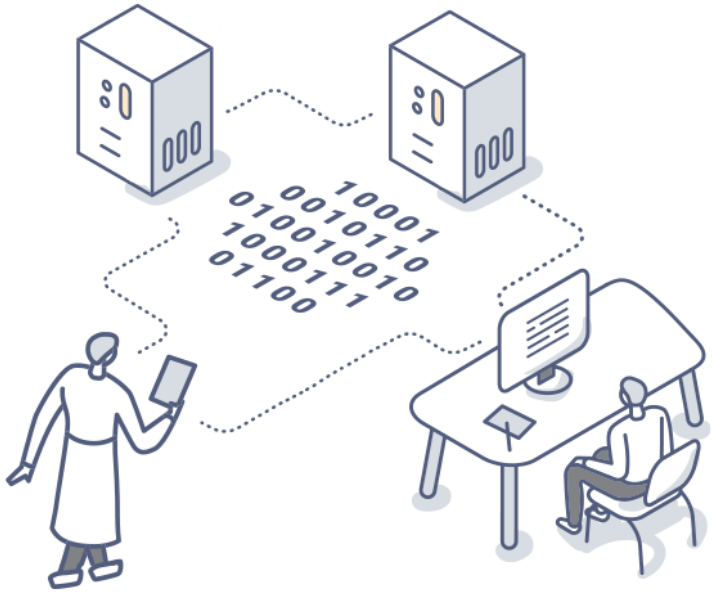
- Research from a 2018 study shows that the use of mHealth apps increased from 16% in 2014 to about 50% in 2018
- A 2017 study identified at least 84,000 mHealth application developers and over 325,000 mHealth apps, with 30% growth in both numbers over the previous year

<u>Types of healthcare apps</u>:

- Education and training
- Decisions support
- Eligibility
- Inter-organizational workflow
- Data management, analytics and reporting
- Notifications
- Clinician-patient communication
- Clinician-clinician communication
- Scheduling
- Health Care Process Improvements
- Personal Health management

APIs and Healthcare: Why are APIs Attractive Attack Vectors?

- APIs protect a valuable target for healthcare organizations: health data.
- Health data:
  - Highly monetizable by cybercriminals paired with a strong buyers market, especially on the dark web.
  - Stolen health credentials are known to be worth 10 to 20 times the value of credit card numbers.
  - The entire healthcare industry is estimated to be worth about $3 trillion.
  - Medical records have been sold on the black market for as much as $1,000 each.
  - Why? Because it's easy to use Personally Identifiable Information (PII) and Personal Health Information (PHI) for fraudulent purposes.
- The ubiquitous nature of APIs combined with the value of health data have made APIs 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 three common types of API protocols:

REST – Stands for **RE**presentative **S**tate **T**ransfer, and is a web services API that provides a uniform interface. Communications occur via the Hypertext Transfer Protocol (HTTP), by using Uniform Resource Identifiers (URIs), the common Create, Read, Update, and Delete (CRUD) operations, and most often JavaScript Object Notation (JSON) conventions for data exchange. REST does not have an official standard but instead uses various protocols.

SOAP – Stands for **S**imple **O**bject **A**ccess **P**rotocol and is another type of web services API. SOAP also leverages HTTP in addition to XML (Extensible Markup Language) for communications, as well as CRUD operations. SOAP APIs are stricter and more heavyweight than REST.

RPC – Stands for **R**emote **P**rocedural **C**all and is the oldest and simplest type of API protocol. RPC is a request-response protocol. A client sends a request to a remote server to execute a specific procedure, and the response is sent back. REST represents server-side data in simple formats such as JSON and XML. RPC APIs are much more challenging to maintain and update than REST APIs and are not implemented as frequently today as they were previously.

REST has become the most common API.

APIs: The Value to the Healthcare Enterprise and Healthcare Consumers

Why do healthcare organizations benefit from APIs?

- Speed – New applications can be developed much quicker if existing APIs allow them to communicate. Having a library of reusable APIs speeds up application development and ongoing app evolution.
- Efficiency – Storage on endpoint systems can be saved and data exchanges can remain open and standardized across various data structures.
- Security – APIs can enable you to more securely expose systems of record and business logic to mobile, web, and cloud apps.
- Marketing/Monetize – Publishing APIs can expand your brand and enable you to tap into broader developer and partner ecosystems to drive innovation. You can also enable new business channels by charging money for the use of, or rate of use of, the APIs that can access your data and algorithms.

How do healthcare consumers benefit from APIs?

- Comprehensiveness – Access to more personal health data.
- Convenience – Greater access to data and care simultaneously.
- Security – Reduction of risk by limiting access to data.
- Speed – Prompt access to data.

Examples of Healthcare APIs

Here are examples of health-related APIs, along with their type:

API Name	Description	Category	Followers	Versions
Chronomics Bio	The Chronomics bio data API enables users to order a range of health tests including COVID-19 tests and receive results back. API methods are available to manage orders, tests, and labs. Chronomics...	Health	0	REST v1
Datachip COVID-19 Vaccine Status For Brazil	Vaccination Status API unifies endpoints and data models across vaccination status APIs from different countries and provider so that you can code just once and instantly integrate your app with...	Health	1	REST v1.0.0
Datachip COVID-19 Vaccine Status For India	The Datachip COVID-19 Vaccine Status For India provides returns vaccine data from the GHO data webservice, Athena. Vaccination Status API unifies endpoints and data models across vaccination status...	Health	9	REST v1.0.0
Datachip COVID-19 Vaccine Status For USA	The Datachip COVID-19 Vaccine Status For USA provides returns vaccine data from the GHO data webservice, Athena. From the provider: "Vaccination Status API unifies endpoints and data models across...	Health	3	REST v1.0.0
Cerner HealthIntent Maestro	Maestro API combines Cerner and Lumeris technology and services for health systems to help health systems drive provider engagement, provide care management services, enable risk score accuracy and...	Healthcare	1	REST v1
Cerner HealthIntent Longitudinal Plan	Cerner HealtheIntent is a population health management platform that can receive data from any EHR, HIT system, insurance claims, pharmacy benefits and other data sources. The Cerner HealthIntent...	Healthcare	2	REST v1
Cerner HealtheIntent Health Concern	Cerner HealtheIntent is a population health management platform that can receive data from any EHR, HIT system, insurance claims, pharmacy benefits and other data sources. The HealthIntent Health...	Healthcare	3	REST v1
11Sight	11Sight offers video call and chat for customer engagement services. The 11Sight RESTful API enables developers to manage users, calls, call details, passwords, profile information, notifications and...	Video	3	REST v2
Index of sciences	Index of Sciences Ltd is a huge database which provides health & nutritional related articles.	Healthcare	3	REST v1.0
Particle Health	Particle Health API offers access to health records for over 250 million unique patients across the U.S. The API is compliant to FHIR and C-CDA standards and operates in a HIPAA compliant manner. For...	Healthcare	9	REST v1
Influenza Research Database Sequence	Sequence API retrieves of sequence information about flu viral genomes and proteins. Sequence are retrieved in FASTA or JSON output formats with user defined public database and ViPR/IRD annotated...	Health	7	REST v1
Sonde Health	The Sonde Platform Service API includes the Sonde Health Check API which measure the level of wellness/health in a given voice sample. A Respiratory Symptoms Risk score is returned from a voice input...	COVID-19	12	REST v1
Koleman Healthcare	https://thekolemangroupscreen.com/background-check-api	Human Resources	3	REST v1.0

Healthcare organizations should favor applications utilizing APIs that abide by these basic principles:

- **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.
- **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.
- **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 is important to control access to them. When practical, solutions based on reputable and proven authentication and authorization mechanisms, such as OAuth2.0 and OpenID Connect, are recommended.

API Security Recommendations (Part 2)

- **Encryption**: Encryption of traffic is also critical, and the Transport Layer Security (TLS) protocol is recommended for organizations whose APIs routinely exchange sensitive data like 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 (5/20/21).
- **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 that this information is continuously protected and not exposed to anyone or anything that lacks proper authorization. It is critically important information leakage is considered when APIs are initially designed, as well as during any update development.
- **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.

- **Service API Implementation**: Service APIs are a model of API implementation that 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, and 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 is 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.
- **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.

Reference Materials

References

- “Intro to APIs: What Are APIs and What Do They Do?”, Upwork.com, September 26, 2016, https://www.upwork.com/resources/intro-to-apis-what-are-apis
- O'Dowd, Elizabeth,"Why Application Programming Interfaces Are Key for Healthcare", HIT Infrastructure, December 12, 2016, https://hitinfrastructure.com/features/why-application-programming-interfaces-are-key-for-healthcare
- Irving, Frank, "Getting a Handle on APIs and Health IT Interoperability", EHR Intelligence, December 8, 2015, https://ehrintelligence.com/news/getting-a-handle-on-apis-and-health-it-interoperability
- "Health Data APIs: Accessing Patient Records, Medical Surveys, and Clinical Studies", Altexsoft.com, February 23, 2021, https://www.altexsoft.com/blog/health-data-apis/
- Siwicki, Bill, "What you need to know about healthcare APIs and interoperability", Healthcare IT News, April 11, 2019, https://www.healthcareitnews.com/news/what-you-need-know-about-healthcare-apis-and-interoperability
- "The Rise of mHealth Apps: A Market Snapshot", Liquid State, March 26, 2018, https://liquid-state.com/mhealth-apps-market-snapshot/
- "Health Data APIs: Accessing Patient Records, Medical Surveys, and Clinical Studies", Altexsoft.com, February 24, 2021, https://www.altexsoft.com/blog/health-data-apis/
- Nikolova, Stela, "84,000 health app publishers in 2017 – Newcomers differ in their go-to-market approach", Research2Guidance, https://research2guidance.com/84000-health-app-publishers-in-2017/
- "100% of Tested mHealth Apps Vulnerable to API Attacks", HIPAA Journal, February 16, 2021, https://www.hipaajournal.com/100-of-tested-mhealth-apps-vulnerable-to-api-attacks/

References

- "Your medical record is worth more to hackers than your credit card.", Reuters, September 24, 2014, https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
- Stack, Brian, "Here's How Much Your Personal Information Is Selling for on the Dark Web", Experian, December 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
- "What is API management?", Redhat, https://www.redhat.com/en/topics/api/what-is-api-management
- Walkowski, Debbie, "Securing APIs: 10 Best Practices for Keeping Your Data and Infrastructure Safe", F5, August 7, 2020, https://www.f5.com/labs/articles/education/securing-apis--10-best-practices-for-keeping-your-data-and-infra
- Padua, Vince, "Healthcare Cyberthreats: An API-First Approach To Protection", Forbes, December 28, 2020, https://www.forbes.com/sites/forbestechcouncil/2021/12/28/healthcare-cyberthreats-an-api-first-approach-to-protection/
- "Health Data APIs: Accessing Patient Records, Medical Surveys, and Clinical Studies", Altexsoft, February 24, 2021, https://www.altexsoft.com/blog/health-data-apis/
- Scroxton, Alex, "Automation, zero-trust, API-based security priorities for EMEA CISOs", Computer Weekly, April 22, 2021, https://www.computerweekly.com/news/252499676/Automation-zero-trust-API-based-security-priorities-for-EMEA-CISOs
- "API Security Outlook: A Guide to API Security in a Digitally Transformed World", EC-Council, April 21, 2021, https://cisomag.eccouncil.org/api-security-outlook-a-guide-to-api-security-in-a-digitally-transformed-world/

References

- HITC Staff, "Emerging Role of Open APIs in Healthcare: 5 Trends to Know", HIT Counsultant, January 13, 2017, https://hitconsultant.net/2017/01/13/37163/#.YHcHYSWSmUk
- Sinhasane, Shailendra, "How Can APIs Bring Digital Healthcare Transformation?", Mobisoft, Janaury 23, 2019, https://mobisoftinfotech.com/resources/blog/how-can-apis-bring-digital-healthcare-transformation/
- Ikeda, Scott, "Mobile Health Apps Are Exposing PII and PHI via API Vulnerabilities; 23 Million May Be Affected", CPO Magazine, February 23, 2021, https://www.cpomagazine.com/cyber-security/mobile-health-apps-are-exposing-pii-and-phi-via-api-vulnerabilities-23-million-may-be-affected/
- Stead, Alistair, "An Introduction to Service APIs", Inviqa, March 18, 2014, https://inviqa.com/blog/introduction-to-service-apis
- Amoroso, Edward, "Understanding cyber threats to APIs", HelpNet Security, June 5, 2020, https://www.helpnetsecurity.com/2020/06/05/api-security-threats/
- Pompon, Ray, "Make sure you keep an eye on your APIs", HelpNet Security, August 13, 2019, https://www.helpnetsecurity.com/2019/08/13/improving-api-security/
- Novikov, Ivan, "5 Security Challenges to API Protection", Dark Reading, April 24, 2019, https://www.darkreading.com/5-security-challenges-to-api-protection/a/d-id/1334475
- Pompon, Raymond & Vinberg, Sander, "Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem", F5 Labs, August 13, 2019, https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem
- Korolov, Maria, "What you need to know about the new OWASP API Security Top 10 list", CSO, November 14, 2019, https://www.csoonline.com/article/3452747/what-you-need-to-know-about-the-new-owasp-api-security-top-10-list.html

References

- Nelson, Jerry, "Three Factors To Consider In Your Web Application And API Cybersecurity Solution", Forbes, April 7, 2020, https://www.forbes.com/sites/forbestechcouncil/2020/04/07/three-factors-to-consider-in-your-web-application-and-api-cybersecurity-solution/?sh=6c056f685e59
- Talwalker, Ameya, "The Growing Importance of API Security", Cyberdefense Magazine, https://www.cyberdefensemagazine.com/the-growing-importance-of-api-security/
- Campbell, Darryn, "Four Ways to Improve Your Mobile Application Security", Devpro Journal, May 11, 2021, https://www.devprojournal.com/technology-trends/mobility/four-ways-to-improve-your-mobile-application-security/
- "Healthcare apps - One of the Most Profitable Mobile Development Trends", Applikey Editorial Team, March 26, 2019, https://applikeysolutions.com/blog/healthcare-apps-one-of-the-most-profitable-mobile-development-trends

Questions

Upcoming Briefs

- Next briefing on June 3rd

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV