Open-Source Software (OSS) Risks in the Health Sector

December 7, 2023

Agenda

- Background on Open-Source Software
- Pros and Cons of Open-Source Software
- Open-Source Software in Healthcare
- Case Studies in Healthcare
- Threats Leveraging Open-Source Software
- Open-Source Software Security
- Major Takeaways

Slides Key:

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

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

Background on OSS

What is Open-Source Software (OSS)?

Note: This briefing will use the acronym OSS for open-source software.

- Open-source software is a field of software development in which the source code for tools, projects, and programs is made freely available to download, modify, and share.
- The complete source code is usually posted publicly via code-sharing platforms like GitHub, allowing anyone to examine it and make changes.
- Common examples include FireFox and Linux.

Image source: Eyes Down Digital

History of Open-Source Software (OSS)

- The roots of open source lie in the origins of software and in computing itself. First pioneered by scientists, researchers and academics, the field was predicated on the free and open sharing of knowledge and information.
- As software development became more commercialized, and competition amongst developers increased, the prevalence of open-source code saw a decline. Despite this, hobbyists have continued the tradition of writing open-source software, even as giant software firms have dominated the sector.

Recent Guidance and Frameworks

- **October 2023**: FDA finalizes guidance mandating that all medical devices running software must create and maintain a software bill of materials (SBOM), including for open-source software.
- **September 2022**: S.4913 - Securing Open Source Software Act of 2022 was introduced to the Senate.
- **February 2022**: NIST Special Publication (SP) 800-218, Secure Software Development Framework (SSDF) v1.1
- **May 2021**: NIST Software Supply Chain Security Guidance from Executive Order (EO) 14028, Section 4

Image source: NIST

How Prevalent is Open-Source Software?

- OSS is part of the foundation of software used to support every single critical infrastructure sector and every National Critical Function (NCF).
- One study found that 96% of studied codebases across various sectors contain open-source code, and 76% of code in studied codebases was open source, according to Synopsis.

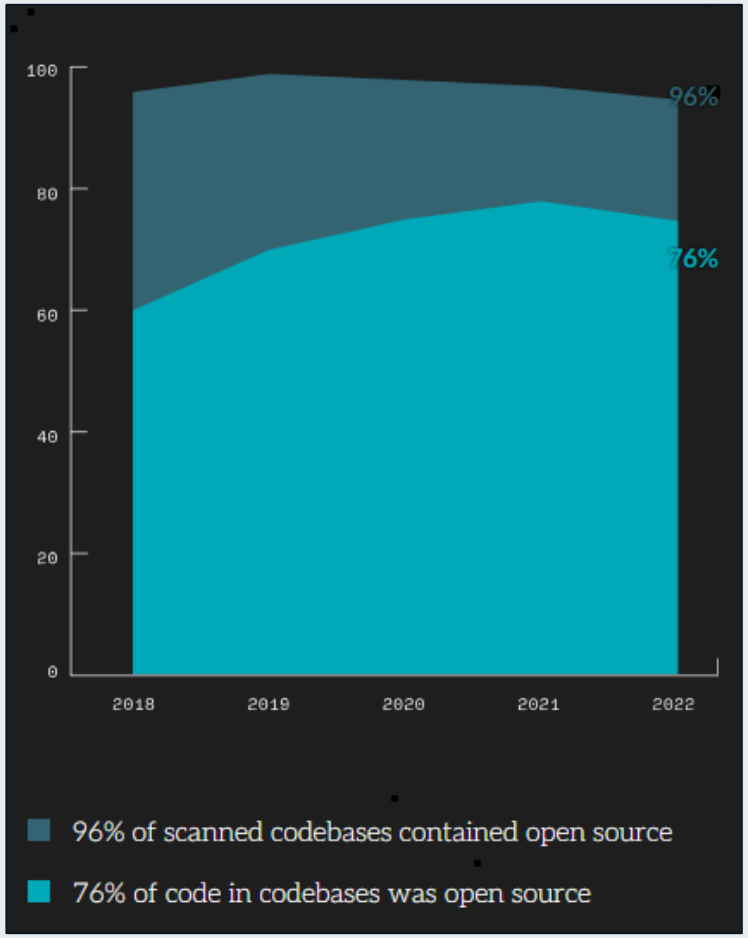


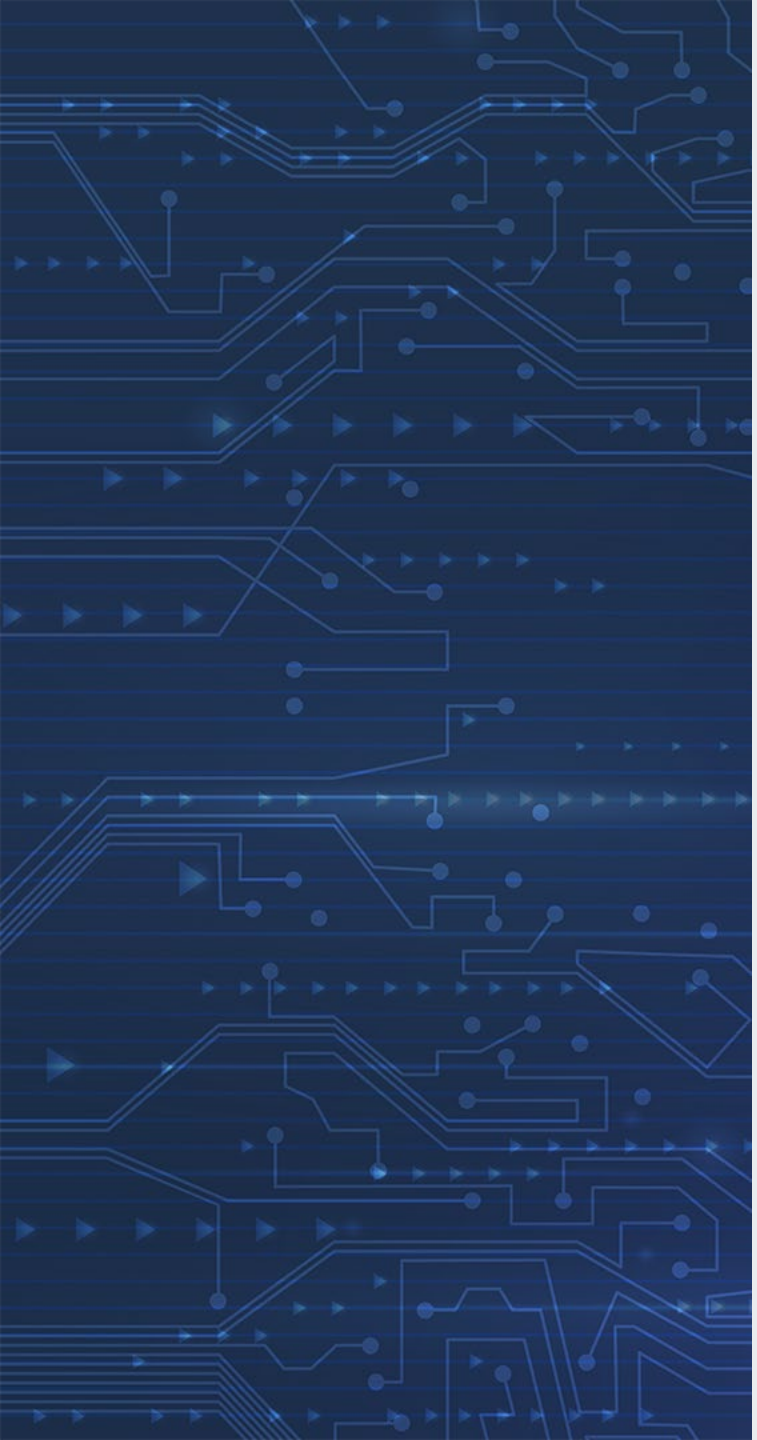
Image source: Synopsys

Benefits of Open-Source Software (OSS)

- Lower starting costs
- Faster project starts
- Faster iteration
- More flexible software development processes
- Robust community-driven support
- Increased feedback and collaboration
- Easier license management

OSS: A Double-Edged Sword

- While open-source software is the bedrock of modern software development, it is also often the weakest link in the software supply chain.
- Known vulnerabilities, compromise of legitimate packages, and name confusion attacks were among the top ten open-source software risks in 2023, according to a report by Endor Labs.



Concerns with OSS

Publicly Accessible Code and Vulnerabilities

- Many eyes on open-source code does not mean people are checking for vulnerabilities or security issues.
- If the source code of software is put in the public domain, it can be accessed by anyone. While this is generally a good thing, bad actors can also access the code to look for vulnerabilities.
- Vulnerabilities in open-source libraries may be embedded into thousands of applications, thereby weakening supply chains with even a single line of code.

Constant Updates Are Necessary

- Open-source code is frequently updated and can quickly become outdated. If code is not regularly updated when updates are made available, security vulnerabilities may go unaddressed.
- It is common for developers to incorporate open-source components in applications and then never update the code.
- Oftentimes, organizations fail to track where open-source code has been used and are completely unaware of any components that need updating.

Lack of Testing and Accountability

- Open-source projects typically lack centralized quality control, resulting in no guarantee that the code has been rigorously tested for security flaws.
- There is limited vendor accountability, and so unlike commercial software vendors who often provide dedicated support, open-source projects tend to lack the structure or resources required to take accountability for security issues.

Open-Source Software (OSS) in Healthcare

Industry Exposure to Open-Source Code

- According to researchers, there is a large and increasing percentage of codebases containing open-source code over time in the Healthcare, Health Tech, and Life Sciences industries from 2018 to 2022, from around 65% in 2018 to roughly 80% in 2022.
- While there was a decrease over time from 2019 to 2021 in the percentage of codebases containing high risk vulnerabilities in the health sector from around 80% to 40%, this number is on the rise again.

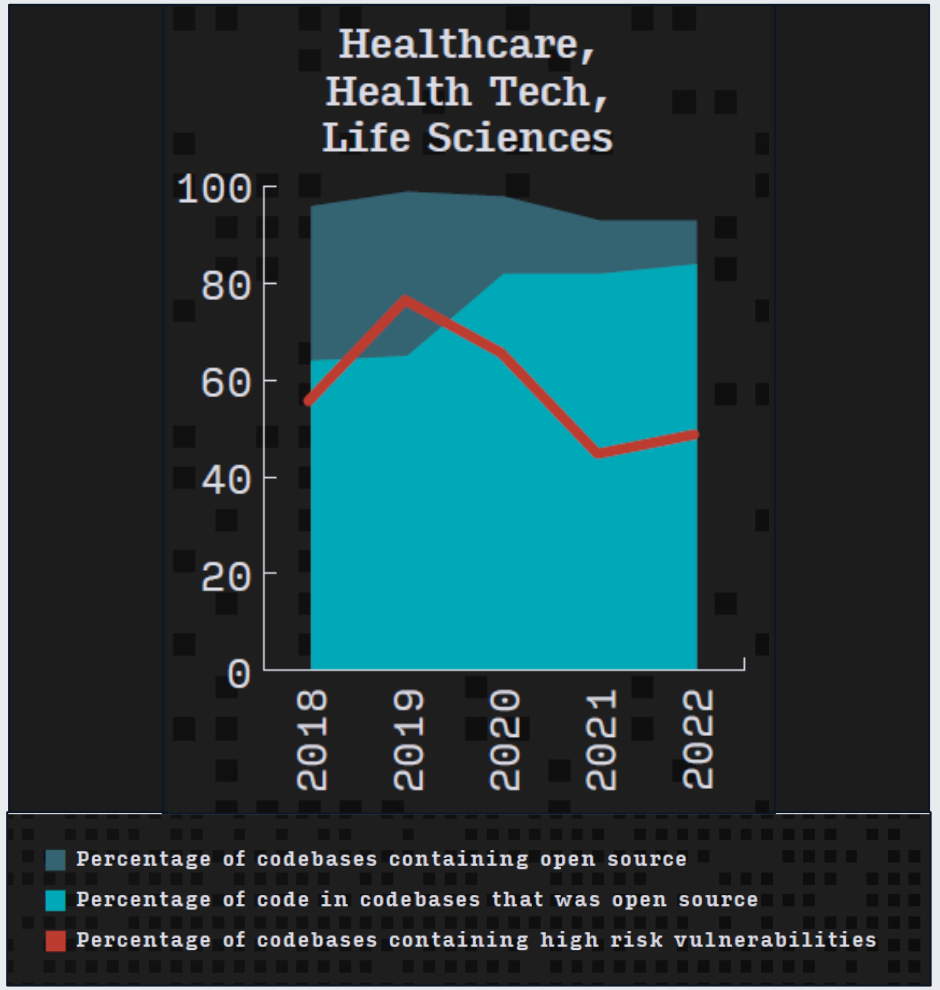


Image source: Synopsys

Examples of OSS in the Health Sector

- Electronic Medical Records (EMR) software:
  - OpenEMR, OpenMRS, OpenClinic, RPMS
- Inventory Management:
  - HospitalRun, MedSupply, SurgiCare Inventory
- Prescription Software:
  - OPENeP, Open Hospital, PatientOS
- Laboratory Management:
  - OpenLIMS, FreeLIMS,
- Clinic Management:
  - OpenClinic, Mr Tooth, OpenEMR
- Medical Billing:
  - OpenEMR, MedManage, OpenPMS

Threats to Medical Devices with OSS

- No documented cyberattacks directly targeting medical devices to-date, however systems encrypted by ransomware attacks often take x-ray machines and other medical devices offline.
- Hacking medical devices with open-source code, such as certain insulin pumps and implanted cardioverter defibrillators, can cause damage to the operation of the medical device.
- Some other examples of medical devices that have used open-source code include defibrillators, ventilators, and the Open Artificial Pancreas System (OpenAPS) project.
- Developing countries are likely to be more saturated with open-source medical devices due to cost and ease-of-use.

Image source: MedCity News

Case Studies in the Health Sector

Prior OSS Vulnerabilities in Healthcare

- **August 2014**: Heartbleed, a major flaw in the OpenSSL encryption technology used in an estimated two-thirds of websites, left networks vulnerable to eavesdropping and data theft, impacting many industries including healthcare. One health system suffered a data breach affecting 4.5 million patients because of the flaw.
- **August 2020**: Numerous zero-day vulnerabilities in an open-source integrated information management system at a hospital exposed patients' test results. Developers were unresponsive to the reports, and users were urged to stop using the program through which unauthenticated attackers could successfully request files containing sensitive documents, including medical test results.

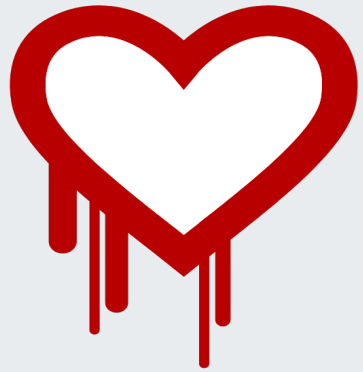


Image source: TechCrunch

Relevant HC3 Resources:

- Nov. 2021: HC3 Threat Brief on Zero Day Attacks (slide 13)

Prior Vulnerabilities: Log4j

- December 2021: The Apache Log4j Project (which is among the most deployed pieces of open-source software, providing logging capabilities for Java applications) was determined to be compromised by a Log4Shell bug, which could allow attackers to access sensitive information, deploy ransomware, and take over vulnerable devices. Various state-sponsored threat actors (including HAFNIUM, PHOSPHOROUS, and APT35) and cybercriminal actors (such as Conti) were observed leveraging these vulnerabilities with medical devices at heightened risk of exploitation.

Image source: Apache

Relevant HC3 Resources:

- Jan 2022: Threat Brief - Log4J Vulnerabilities and the Health Sector

Prior Vulnerabilities: OpenEMR

- January 2023: Multiple vulnerabilities were found in the popular OpenEMR electronic health records system, which could allow for an attacker to access sensitive information, and even compromise the entire system. OpenEMR was described as “used by more than 100,000 medical providers serving more than 200 million patients.” The three vulnerabilities involved Unauthenticated File Read, Authenticated Local File Inclusion, and Authenticated Reflected XSS.

Image source: open-emr.org

Relevant HC3 Resources
- Jan 2023: HC3 Sector Alert on OpenEMR

Case Studies in Other Industries

Recent OSS Supply Chain Attacks in Banking

- Open-source software supply chain attacks that specifically targeted the banking sector but are still applicable to the healthcare industry.
- These attacks leveraged trust placed in commonly used components and showcased advanced techniques, with the attackers employing deceptive tactics.
- The malicious open-source packages have been reported on by researchers and removed. However, researchers still predict a persistent trend of attacks against the banking sector's software supply chain to continue.
- Current controls aimed at detecting and managing known vulnerabilities fall short in countering these new attacks. Industry-wide collaboration is essential to strengthen our defenses against these attacks.

Image source: Techfunnel

North Korea Weaponizing Open-Source Software

- Beginning April 2022, Diamond Sleet, a sub-group of the North Korean Lazarus hacking group, which has some overlap with TEMP.Hermit, had implanted malicious payloads in open-source software to infiltrate corporate networks.
- MSTIC observed Diamond Sleet weaponizing a wide range of open-source software, including PuTTY, KiTTY, TightVNC, Sumatra PDF Reader, and muPDF/Subliminal Recording software installer, for attacks which targeted employees in organizations across multiple industries, including media, defense and aerospace, and IT services in the United States, the United Kingdom, India, and Russia.
- The threat actor was observed attempting to move laterally and exfiltrate collected information from victim networks.

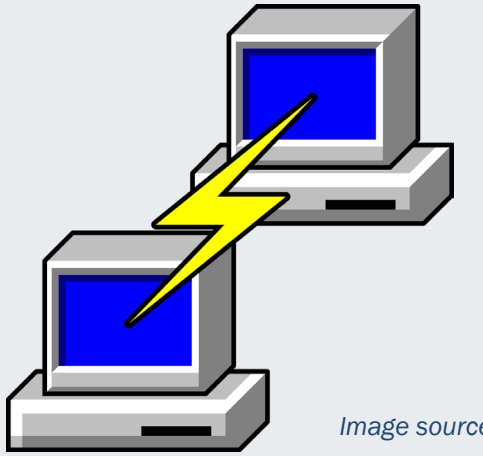
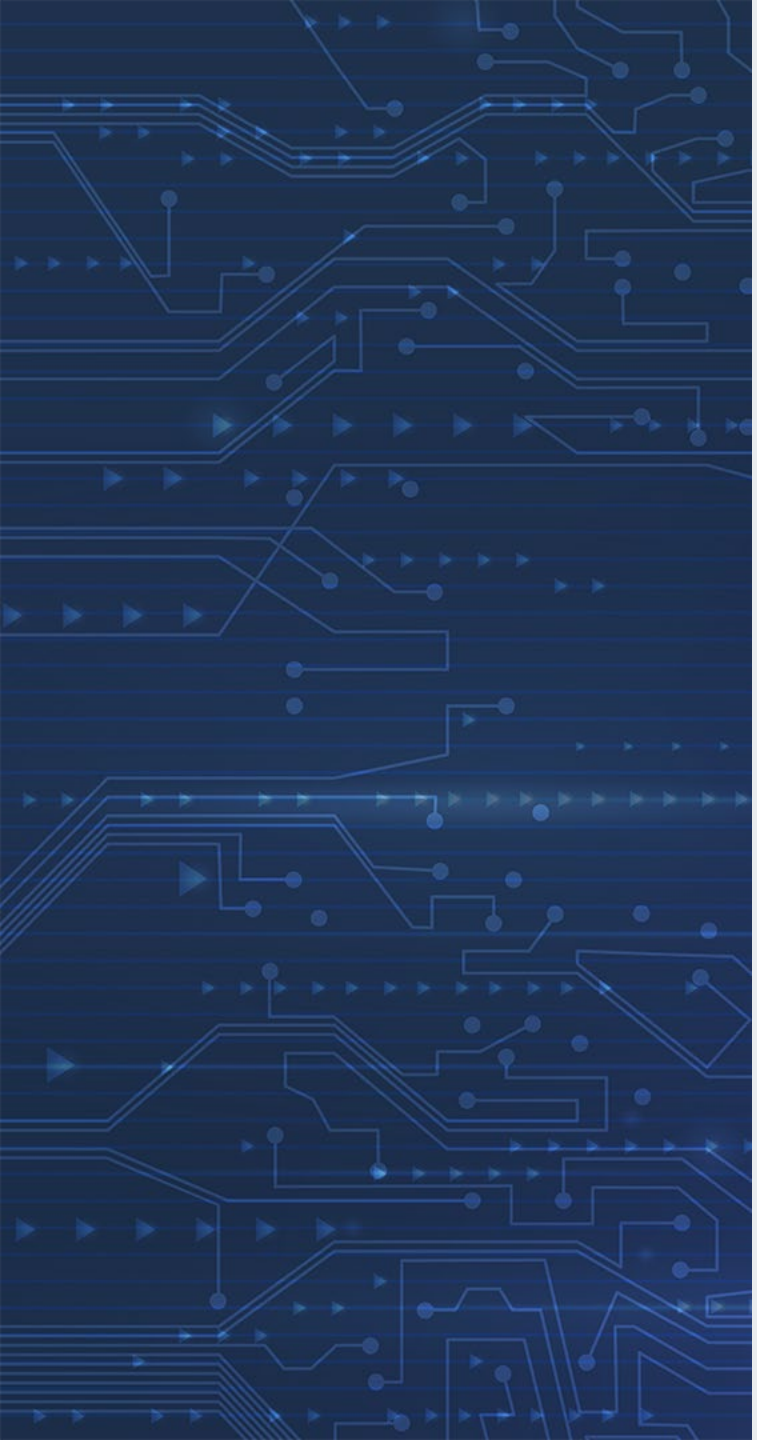


Image source: MIT

Open-Source Tools Used in Attacks

Case Study: SapphireStealer

- SapphireStealer: Open-source information stealer observed across public malware repositories, with increasing frequency since its initial public release in December 2022.
- Information-stealing malware like SapphireStealer can be used to obtain sensitive information, including corporate credentials, which are often re-sold to other threat actors who leverage the access for additional attacks, including operations related to espionage or ransomware/extortion.
- In some cases, SapphireStealer appears to be delivered as part of a multi-stage infection process, with threat actors leveraging open-source malware downloaders like FUD-Loader to deliver SapphireStealer to potential victims.



Cybersecurity Risks and OSS Repositories

Open-Source Software Repositories

Some examples of open-source software repositories include:

- **npm**: Stands for Node Package Manager. It is a library and registry for JavaScript software packages. npm also has command-line tools to help you install the different packages and manage their dependencies. npm is free and relied on by over 17 million developers worldwide.
- **NuGet**: Open-source package manager and software distribution system, enabling developers to download and include ready-to-run .NET libraries for their projects.
- **PyPI**: The Python Package Index, abbreviated as PyPI and also known as the Cheese Shop, is the official third-party software repository for Python.

Malicious Campaigns with OSS Repositories

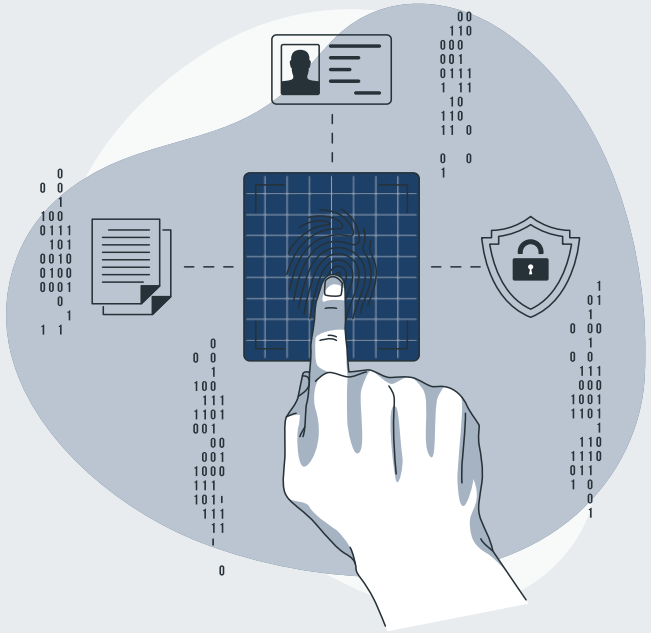
Recent malicious campaigns leveraging open-source software repositories:

- **August 2023**: "VMConnect" malicious supply chain campaign with dozens of malicious Python packages posted to PyPI open-source repository, with links to Labryinth Cholima/Lazarus Group.
- **September 2023**: SSH keys stolen by stream of malicious PyPI and npm packages.
- **October 4, 2023**: Researchers discover that one “s” was all that separated a legit npm package from a malicious twin that delivered the r77 rootkit, downloaded more than 700 times.
- **October 15, 2023**: Malicious NuGet packages abuse MSBuild to install malware.
- **April–October 2023**: 272 packages with code for stealing sensitive data from targeted systems planted on open-source platforms receive 75,000 downloads.
- **November 2023**: A threat actor was caught planting malicious Python packages into an open-source repository for nearly half a year, which received thousands of downloads.
- **November 2023**: Newly discovered OSS packages on the npm platform contain scripts that broadcast peace messages related to ongoing conflicts in Ukraine and Gaza.

Malicious Package Infection Methods

Types of malicious package infection methods:

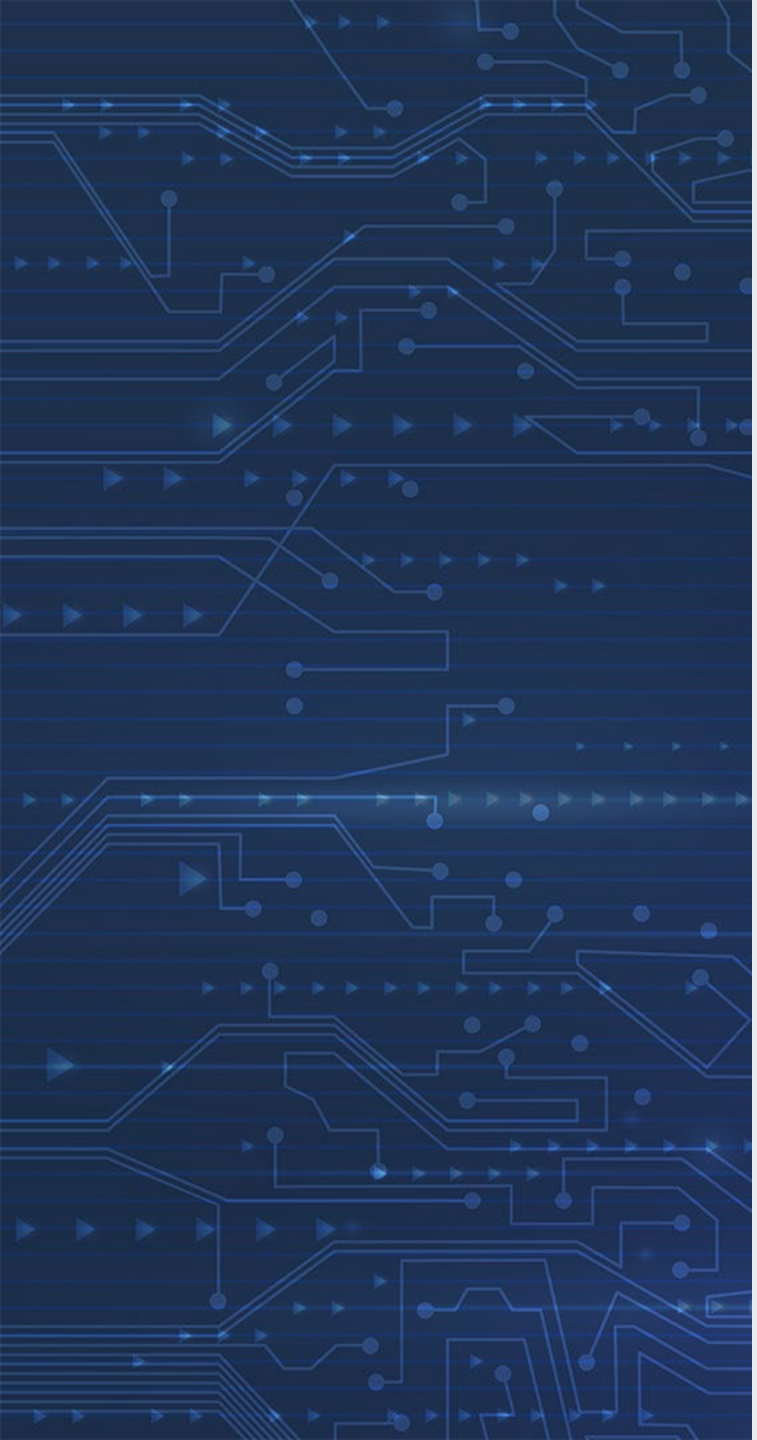
- **Typosquatting**: Typographical errors used in malicious package names to resemble popular packages with the goal of tricking victims.
- **Masquerading**: Code and metadata of known packages are duplicated, and malicious code is added, creating a Trojan package.
- **Dependency Confusion**: A valid name of an internal package for the malicious package is published on a public repository with higher version numbers.
- **Dependency Hijacking**: A legitimate package is compromised and implanted with malicious code.



Mitigations for Malicious Package Attacks

Some best practices to prevent malicious package attacks include:

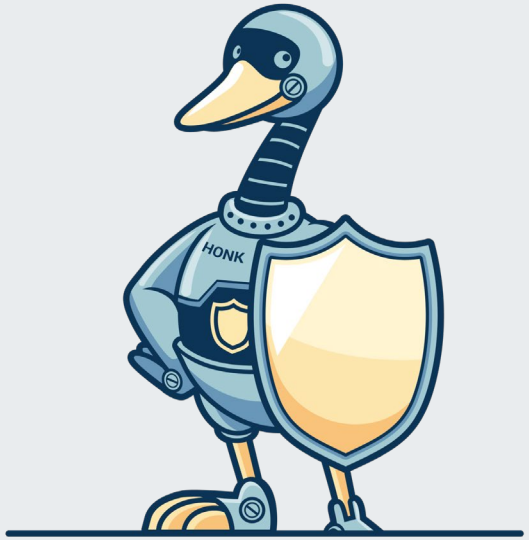
- Verify package ownership and authenticity
- Scan packages
- Inspect DNS settings
- Check functionality changes
- Perform code reviews
- Verify package checksums



Open-Source Security

Open Source Security and SLSA

- Open Source Security is a methodology to provide users better visibility into the open-source inventory of their applications.
- The Open Source Security Foundation (OpenSSF) is a cross-industry forum for a collaborative effort to improve open-source software security.
- OpenSSF announced the release of Supply-chain Levels for Software Artifacts (SLSA) v.1.0 in April 2023.



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Image source: OpenSSF

Evaluating Open-Source Software (OSS)

According to SonaType, an evaluation entails:

- scrutinizing the development methodology;
- gauging the project community's activity;
- analyzing the codebase's security, particularly in terms of open-source vulnerabilities; and
- assessing the open-source project maintainer's level of involvement and responsiveness to security issues serves as an important element for review.

Software Bill of Materials (SBOMs)

- Lists all components and dependencies that make up a piece of software, which helps identify potential vulnerabilities.
- Provides transparency into a software supply chain to help manage security and compliance risks.
- Many open-source projects already provide an SBOM as part of their release process, and some organizations are requiring the use of SBOMs as a condition of using open-source software.

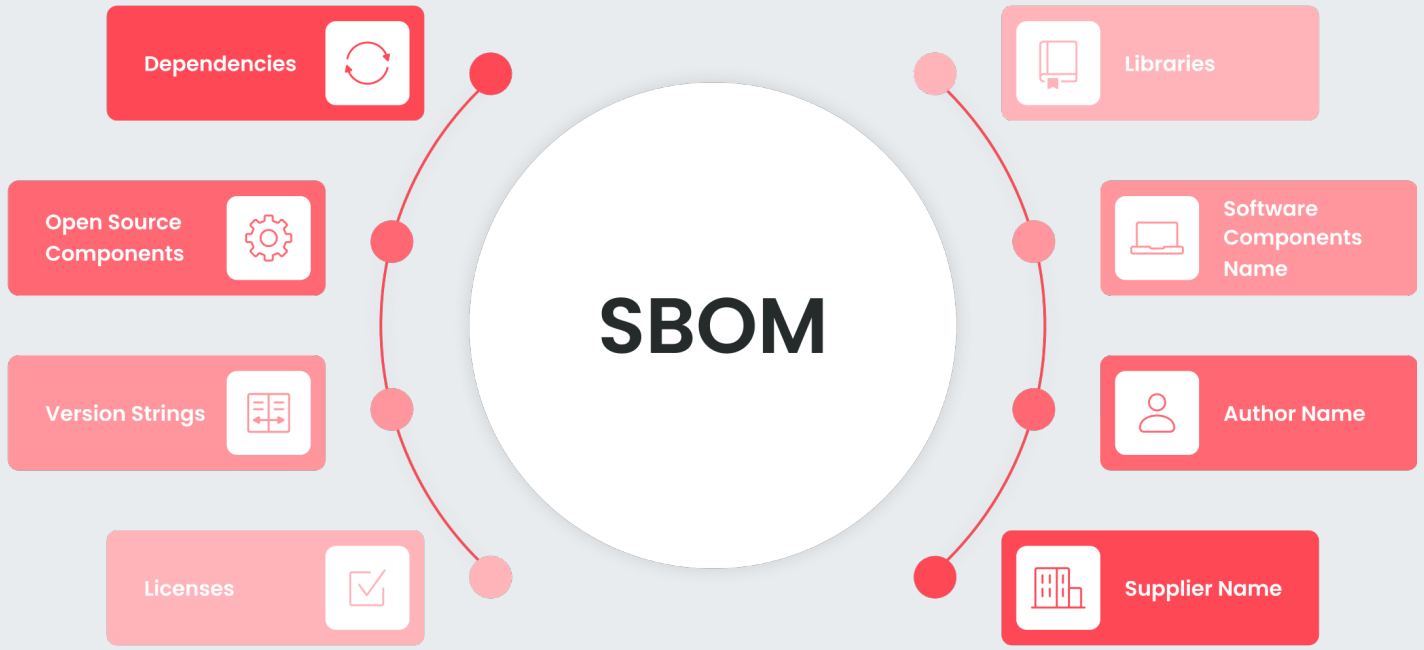


Image source: Replicated.com

Software Composition Analysis (SCA)

- Software composition analysis (SCA) is an automated process that identifies the open-source software in a codebase.
- SCA tools can also be used to generate a software bill of materials (SBOM) that includes all the open-source components used by an application.
- Leveraging integrated development environments (IDEs) plugins, SCA tools can notify developers about vulnerabilities as they add packages.

Software Composition Analysis (SCA), cont.

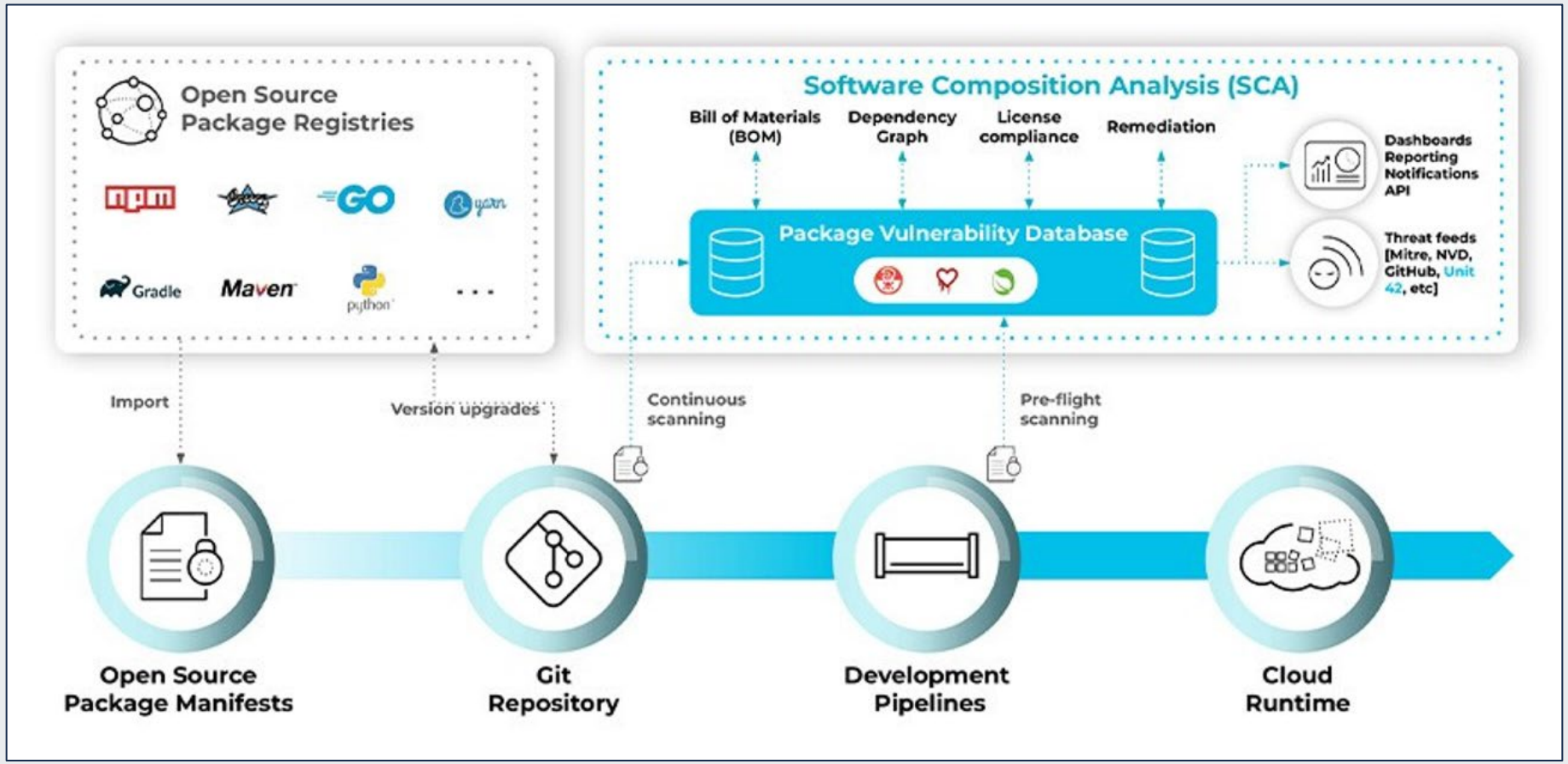


Image source: Palo Alto Networks

CISA Open Source Software Security Roadmap

- Released on September 12, 2023 at TLP:CLEAR
- Four key goals: 1) establishing CISA's role in supporting the security of OSS, 2) understanding the prevalence of key open-source dependencies, 3) reducing risks to the federal government, and 4) hardening the broader OSS ecosystem.
- CISA is broadly concerned about two distinct classes of OSS vulnerabilities and attacks:
  - The cascading effects of vulnerabilities in widely-used OSS.
  - Supply-chain attacks on open-source repositories leading to compromise of downstream software.
- Link: CISA Open Source Software Security Roadmap

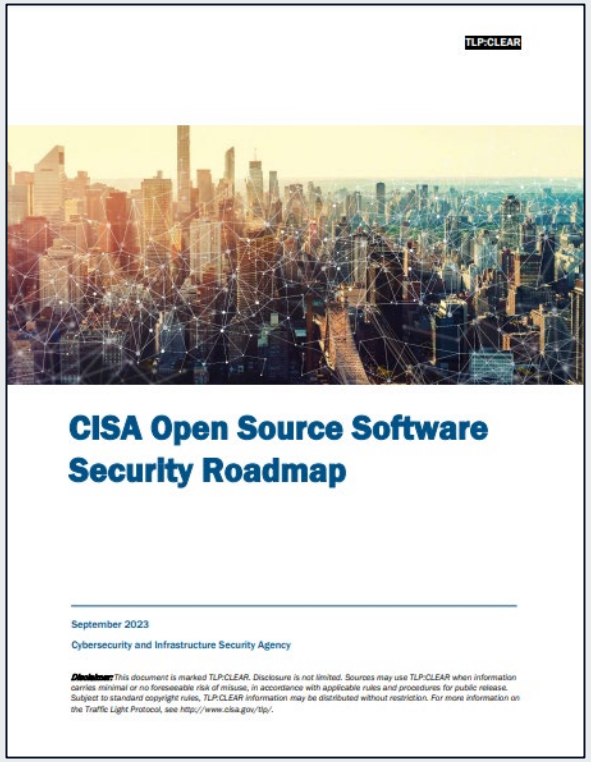
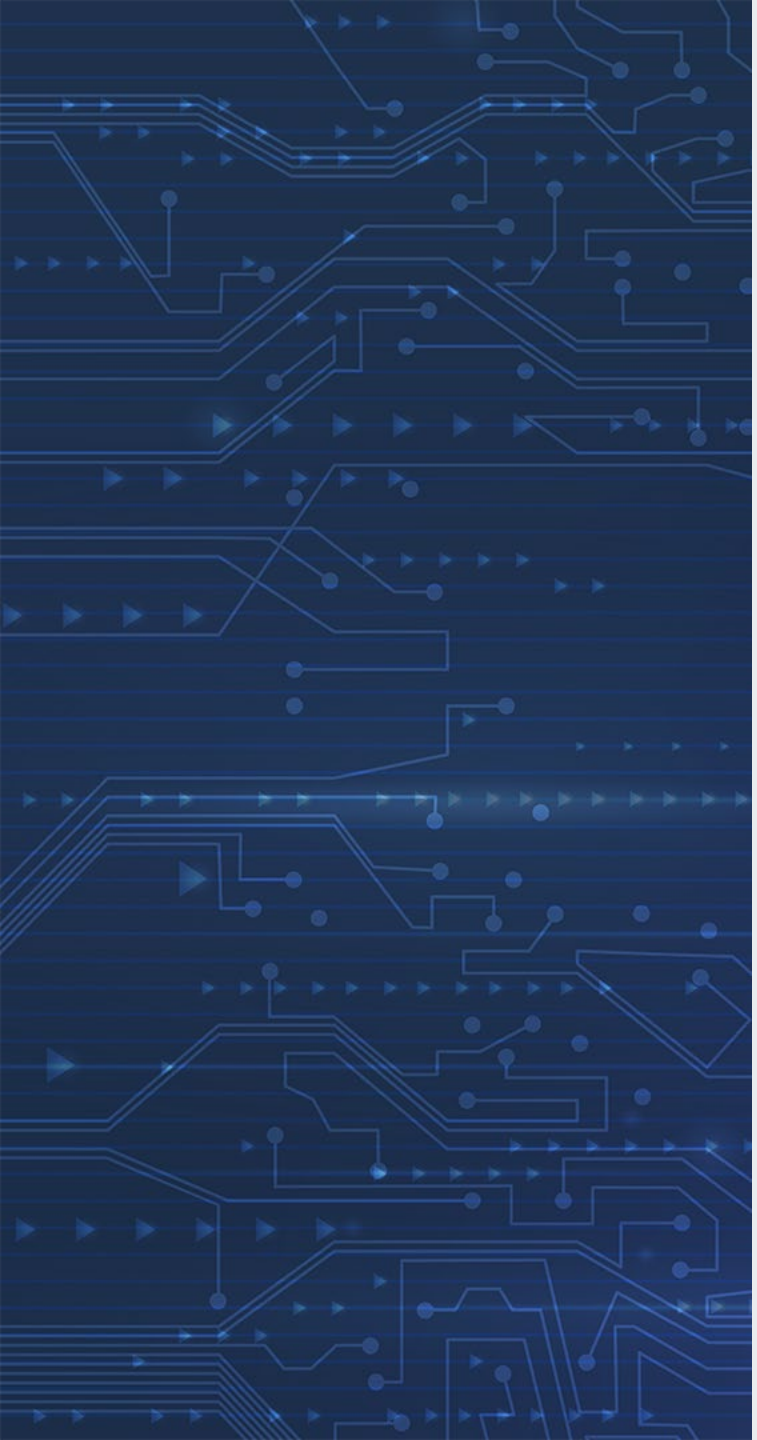


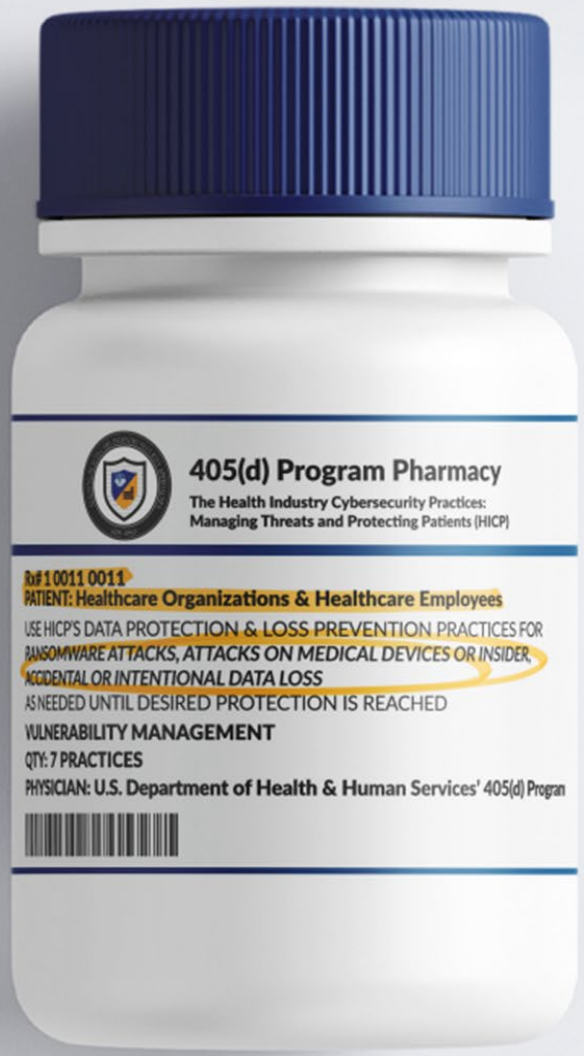
Image source: CISA



Conclusion

Major Takeaways

- Proprietary software may contain open-source code.
- Previous high-profile attacks in the health sector involving open-source code include Heartbleed and Log4j.
- State-sponsored threat actors have implanted malicious payloads in open-source software to infiltrate corporate networks.
- Software Bill of Materials (SBOMs) and Software Composition Analysis (SCA) are an important step towards open-source security.



PRESCRIPTION:

Vulnerability Management

Vulnerability management is the process used by organizations to detect technology flaws that hackers could exploit. This process uses a scanning capability, often provided by an EHR or IT support vendor, to proactively scan devices and systems in your organization.

Protect yourself and your patients by following the course of treatment below:

For Small Organizations:

- Schedule and conduct vulnerability scans on servers and systems under your control to proactively identify technology flaws.
- Conduct web application scanning of internet-facing webservers, such as web-based patient portals. Specialized vulnerability scanners can interrogate running web applications to identify vulnerabilities in the application design.
- Conduct routine patching of security flaws in servers, applications (including web applications), and third-party software. Maintain software at least monthly, implementing patches distributed by the vendor community, and always patch critical vulnerabilities within 14 days.

For Medium/Large Organizations:

In addition to instituting the tips for Small Organizations be sure to incorporate the following:

- Implement Host/Vulnerability Endpoints Scanning. In this model, vulnerability scanners are leveraged to identify weaknesses in OS or third-party applications that reside on endpoints and servers.
- Utilize strict configuration management and change management procedures. Also, a testing plan should be part of the change management process. It should include a vulnerability scan of new network connectivity (such as a firewall change) or a new system function or service.
- Establish a routine of penetration testing. These types of tests are sometimes called red teaming; the goal is to actively exploit your own environment before malicious actors do.

*For more Vulnerability Management practices, please visit **405d.hhs.gov** to download a copy of the HICP technical volume for your organization. Check out the available resources 405(d) has to offer by visiting our social media pages @ask405d on Facebook, Twitter, and Instagram!*

Reference Materials

References

- Top 10 open source software risks for 2023. Apurva Venkat. March 1, 2023. https://www.csoonline.com/article/3688924/top-10-open-source-software-risks-for-2023.html
- Our Medical Devices' Open Source Problem – What Are the Risks?. Cybellum. May 11, 2022. https://www.bleepingcomputer.com/news/security/our-medical-devices-open-source-problem-what-are-the-risks/
- Vetting the Security Risks of Open-Source Code in Healthcare. Marianne Kolbasuk McGee. January 28, 2022. https://www.govinfosecurity.com/interviews/vetting-security-risks-open-source-code-in-healthcare-i-5017
- Open Source Security Risks. https://www.hipaajournal.com/open-source-security-risks/
- Addressing Cybersecurity Challenges in Open Source Software: What you need to know. Ashwin Ramaswami. September 1, 2022. https://www.linuxfoundation.org/blog/blog/addressing-cybersecurity-challenges-in-open-source-software-what-you-need-to-know

- 5 free or open-source healthcare software tools ready to serve and help heal. Jack Wallen. December 2, 2021. https://www.techrepublic.com/article/five-free-or-open-source-healthcare-software-tools-ready-to-serve-and-help-heal/
- Why Open Source Security Matters for Healthcare Orgs. Elizabeth Snell. October 18, 2017. https://www.techrepublic.com/article/five-free-or-open-source-healthcare-software-tools-ready-to-serve-and-help-heal/
- Top 10 open source software risks for 2023. Apurva Venkat. March 1, 2023. https://www.csoonline.com/article/3688924/top-10-open-source-software-risks-for-2023.html
- Top 10 Open Source Software (OSS) Risks. https://www.endorlabs.com/top-10-open-source-risks
- Serious Vulnerabilities identified in the OpenClinic GA Integrated Hospital Information Management System (July 3, 2020). https://www.hipaajournal.com/serious-vulnerabilities-identified-in-the-openclinic-ga-integrated-hospital-information-management-system/

- Electronic Medical Records Cracked Open by OpenClinic Bugs. Seals, Tara. December 1, 2020. https://threatpost.com/electronic-medical-records-openclinic-bugs/161722/
- What is open source? McCallion, Jane. June 30, 2022. https://www.itpro.com/software/28109/what-is-open-source
- The Friday Dive: Community Health breach caused by Heartbleed bug. Williams, Katie Bo. August 22, 2014. https://www.healthcaredive.com/news/the-friday-dive-community-health-breach-caused-by-heartbleed-bug/300580/
- Impact of New US National Cybersecurity Strategy on Organizations Building With OSS (March 10, 2023). https://solutionsreview.com/network-monitoring/impact-of-new-us-national-cybersecurity-strategy-on-organizations-building-with-oss/
- A guide for open source software (OSS) security. Linskens, Aaron. August 28, 2023. https://blog.sonatype.com/a-guide-for-open-source-software-oss-security

- Why the FDA's SBOM Mandate Changes the Game for OSS Security. Gile, Jenn. June 27, 2023. https://www.darkreading.com/attacks-breaches/fda-sbom-mandate-changes-oss-security
- What is Open Source Security? Checkpoint. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-open-source-security/
- Managing Open Source Security Risks and Vulnerabilities. Jfrog. June 12, 2023. https://jfrog.com/devops-tools/article/managing-open-source-security-risks-and-vulnerabilities/
- What Is Software Composition Analysis (SCA)? Palo Alto. https://www.paloaltonetworks.com/cyberpedia/what-is-sca
- Making Open Source software safer and more secure. Walker, Kent. January 13, 2022. https://blog.google/technology/safety-security/making-open-source-software-safer-and-more-secure/

- Sensitive Data Exfiltration Campaign Targets npm and PyPI. Phylum Research. September 26, 2023. http://blog.phylum.io/sensitive-data-exfiltration-campaign-targets-npm-and-pypi/
- npm packages caught exfiltrating Kubernetes config, SSH keys. Sharma, Ax. September 19, 2023. https://blog.sonatype.com/npm-packages-caught-exfiltrating-kubernetes-config-ssh-keys
- Hundreds of malicious Python packages found stealing sensitive data. Toulas, Bill. October 4, 2023. https://www.bleepingcomputer.com/news/security/hundreds-of-malicious-python-packages-found-stealing-sensitive-data/
- Typosquatting campaign delivers r77 rootkit via npm. Reversing Labs. October 4, 2023. https://www.reversinglabs.com/blog/r77-rootkit-typosquatting-npm-threat-research
- Malicious NuGet packages abuse MSBuild to install malware. Toulas, Bill. October 31, 2023. https://www.bleepingcomputer.com/news/security/malicious-nuget-packages-abuse-msbuild-to-install-malware/

- Attacker – hidden in plain sight for nearly six months – targeting Python developers. Gelb, Yehuda. November 16, 2023. https://checkmarx.com/blog/attacker-hidden-in-plain-sight-for-nearly-six-months-targeting-python-developers/
- Protestware taps npm to call out wars in Ukraine, Gaza. Roberts, Paul. November 16, 2023. https://www.reversinglabs.com/blog/protestware-taps-npm-to-call-out-wars-in-ukraine-gaza

Questions

FAQ

Upcoming Briefing

- 1/18/24 – Ransomware & Healthcare

Product Evaluations

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

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

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. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and 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.

Alerts and Analyst Notes

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

Threat Briefings

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.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV