SECURING THE OPEN-SOURCE SOFTWARE ECOSYSTEM

END OF YEAR REPORT: OPEN-SOURCE SOFTWARE SECURITY INITIATIVE (OS3I)

JANUARY 2024

THE WHITE HOUSE
WASHINGTON

Table of Contents

EXECUTIVE SUMMARY

Since the discovery of the Log4Shell vulnerability in 2021, the Biden-Harris Administration has fortified its commitment to secure the open-source software ecosystem.[i] In March 2023, the Biden-Harris Administration released the National Cybersecurity Strategy (NCS), which stated, "*in partnership with the private sector and the open-source software community, the Federal Government will also continue to invest in the development of secure software, including memory-safe languages and software development techniques, frameworks, and testing tools.*"[ii] This commitment laid the foundation for the Office of the National Cyber Director (ONCD) to foster improved security in open-source software development practices through the 2023 NCS Implementation Plan Initiative 4.1.2, "Promote open-source software security and the adoption of memory-safe programming languages."[iii]

The NCS Implementation Plan expands and matures the role of the Open-Source Software Security Initiative (OS3I).[iv] The OS3I convenes Federal agencies and considers input from the open-source software community, civil society, and private sector stakeholders across the open-source software landscape to deliver policy solutions to secure and defend the open-source software ecosystem.

In 2023, OS3I members focused on four key areas:

(1) **Unifying the Federal Government's voice on open-source software security.** The OS3I worked to align the Federal position on open-source software security and coordinate relevant workstreams.

(2) **Establishing a strategic approach for the Federal Government's secure use of open-source software and efforts to secure the broader ecosystem**. The Cybersecurity and Infrastructure Security Agency (CISA), in coordination with the OS3I, released its Open Source Software (OSS) Security Roadmap to build relationships with open-source software communities, measure open-source software prevalence, help secure the usage of open-source software by Federal departments and agencies, and to bolster the overall security of the open-source ecosystem.

(3) **Encouraging long-term, sustained security investment in the open-source software ecosystem**. Advancing President Biden's Invest in America agenda, the OS3I recognizes the importance of encouraging investment in the open-source software ecosystem. The National Science Foundation (NSF), an OS3I member, published a "Dear Colleague Letter" inviting proposals on methods to secure the open-source software ecosystem.

(4) **Engaging and building trust with the open-source software community**. As part of the OS3I, ONCD, CISA, NSF, Defense Advanced Research Projects Agency (DARPA), and Office of Management and Budget (OMB) issued a Request for Information to gather input from the open-source community and focus government priorities on open-source software security, which received over a hundred substantive responses.

This End of Year Report is a product of the OS3I Working Group, established by ONCD pursuant to the NCS Implementation Plan Initiative 4.1.2. The Report begins by providing background on the significance of open-source software, its ecosystem, and inherent challenges. Next, the report recaps

the progress made by the OS3I on key 2023 deliverables in each of the aforementioned key areas. The report concludes with prospects for OS3I work in 2024.

INTRODUCTION

Americans rely on systems that are built on the foundation of open-source software. The benefits of open-source software, including its lower total cost of ownership, ease of adoption, transparency, and composability (i.e., it can be inspected, modified, and enhanced) have helped drive its ubiquity in hardware and software across nearly every economic sector. Almost every software application, website, mobile device, and Internet of Things device—including those used by small businesses, the Federal Government, and the national security community—incorporates open-source software to enable and scale rapid application development processes.

Due to open-source software's widespread use, software vulnerabilities in open-source software can have exceptionally broad impacts across commercial products and downstream users. Just as with proprietary software, it is essential to establish secure software development, vulnerability management, and vulnerability disclosure practices for open-source software. However, because open-source software development is often decentralized and volunteer-driven, adoption of best- practices is not uniform. Further, the pervasiveness of open-source software within software packages, combined with its composability, makes it difficult for end-users to identify all of the open-source software within software applications and connected products.

Another challenge is the prevalence of code written in memory-unsafe programming languages, especially in systems-level software (e.g., operating systems), which contributes to critical software vulnerabilities.[v] Memory unsafety is a systemic issue that is common both to open-source and proprietary software. Analysis of publicly-disclosed software vulnerabilities discovered in industry-leading applications suggest that 70% or more were due to memory safety issues.[vi]

Efforts to secure open-source software are challenged by a range of factors, including decisions within companies to reserve security-related features for commercial products built upon open-source software, inconsistent contributions to help sustain open-source software projects from corporate consumers, and the decentralized ownership and varied development processes of open-source projects, with contributions coming from entities with varying resources, capabilities, and priorities. Given that open-source software is a public good, ensuring open-source software's resilience is a technical necessity and a strategic imperative for protecting and promoting U.S. interests.

2023 ACCOMPLISHMENTS

In 2022, the Biden-Harris Administration expanded its commitment to open-source software security by establishing the OS3I, which will continue its efforts in 2024. The OS3I is a convening of staff-level representatives from select Federal departments and agencies to coordinate policy solutions to better secure and defend the open-source software ecosystem. In 2023, the OS3I focused on four key areas: (1) unifying Federal departments and agencies to speak with a single voice on open-source software security; (2) establishing a strategic approach for the Federal Government's secure use of open-source software; (3) encouraging long-term, sustained security investment into the open-source software ecosystem; and (4) engaging and building trust with the open-source software community. As articulated in the NCS, the Biden-Harris Administration is committed to long-term planning and

collaboration with the open-source software community to achieve a more defensible and resilient digital ecosystem.

1. UNIFYING DEPARTMENTS AND AGENCIES TO SPEAK WITH A SINGLE VOICE ON OPEN-SOURCE SOFTWARE SECURITY:

The OS3I was convened to foster alignment on open-source software security between Federal departments and agencies, industry, academic, and other stakeholders. Recognizing the opportunities for more consistent engagement, ONCD, with support from the OMB Office of the Federal Chief Information Officer (OFCIO), established the OS3I as an interagency staff-level working group to coordinate government efforts to foster open-source software security, including championing memory-safe programming languages.

The OS3I sought feedback from public and private stakeholders to identify opportunities to improve the security of the open-source software ecosystem and any associated risks. The OS3I engaged with and collected input from academia, open-source nonprofits and providers of core open-source infrastructure, including package managers, code hosting services, and philanthropic funders. Further, the OS3I reviewed existing government research and development efforts on open-source software security.

2. ESTABLISHING A STRATEGIC APPROACH FOR THE SECURE USE OF OPEN-SOURCE SOFTWARE:

Vulnerabilities in widely used open-source software libraries create risks to national security, economic security, and public safety. Open-source software is part of the foundation of software used by all sixteen critical infrastructure sectors and every national critical function to support Americans' daily lives.[vii] Increasing the security baseline of open-source software, including that used by critical infrastructure, increases the digital resilience of the Nation and allows the open-source software ecosystem to continue to foster innovation. In September, CISA released its Open-Source Software Security Roadmap to advance its mission of understanding, managing, and reducing risks to the Federal Government and critical infrastructure. CISA's Open-Source Software Security Roadmap serves as an important guide for other departments and agencies–including those that support critical infrastructure–to manage open-source software risks and help secure the broader ecosystem. The Open-Source Software Security Roadmap lays out four goals: (1) establishing CISA's role by building relationships with open-source software communities; (2) understanding open-source software prevalence; (3) reducing risks to the Federal Government; and (4) hardening the open-source software ecosystem.

3. INVESTING RESOURCES IN THE OPEN-SOURCE SOFTWARE ECOSYSTEM:

While the source code for open-source software is made freely available, there are still financial, time, and opportunity costs associated with its use and maintenance, including those for improving its security. The Federal Government is committed to advancing the security of the open-source software ecosystem. As part of this effort to invest in the ecosystem, the NSF released a Dear Colleague Letter (DCL) encouraging submission of proposals targeting software engineering methodologies, unsafe

legacy code, dependency management, trust and safety, incentive and organizational structures, and education and workforce development. The DCL is part of the ongoing, decade-long effort of NSF's Secure and Trustworthy Cyberspace Program to advance software and system security.

4. ENGAGING THE OPEN-SOURCE SOFTWARE COMMUNITY:

The OS3I is committed to engaging the open-source software community, a uniquely diversified and decentralized ecosystem, whose participants range from Fortune 500 companies, to non-profit organizations, to individuals across the globe, all collaborating to develop and maintain software for the common good. Over the past year, the OS3I identified several focus areas to engage the open-source software community, including: (1) fostering the proliferation of memory safe programming languages; (2) fostering sustainable development and utilization of open-source software; (3) bolstering the security of package managers and other centralized infrastructure; and (4) identifying new focus areas to prioritize.

In pursuit of this goal, ONCD, CISA, NSF, DARPA, and OMB released a Request for Information (RFI) on Open-Source Software Security published in the Federal Register in August 2023. It aims to identify areas most appropriate to focus Federal Government open-source software security priorities, and address the following critical questions:

(1) Securing Open-Source Software Foundations
(2) Sustaining Open-Source Software Communities and Governance
(3) Creating Behavioral and Economic Incentives to Secure the Open-Source Software Ecosystem
(4) Improving R&D/Innovation
(5) Expanding International Collaboration

The OS3I received more than one hundred substantive responses from a broad range of representatives in the open-source software community, including open-source software non-profits, individuals, industry, academia, and research organizations. Initial review indicates the majority of submissions referenced solutions for securing open-source software foundations. Other responses focused on solutions to sustain open-source software communities and governance; encourage security research and development; address behavioral and economic incentives to secure the open-source software ecosystem; and promote international collaboration.

In 2024, the OS3I will use the submissions to determine how the Federal Government can drive down the most important systemic risks and foster the long-term sustainability of open-source software communities. The OS3I will publish a summary of the RFI submissions to help consolidate key findings.

CONCLUSION

The OS3I will continue working with the open-source software community to strengthen the ecosystem. A defensible, resilient, and flourishing open-source ecosystem will require further collaboration and coordinated investment from public and private sectors alike. The OS3I's focus on bringing together stakeholders from across the Federal Government with input from the open-source

software community, industry, and civil society aims to push forward key implementation initiatives and amplify ongoing progress. Continued collaboration and investments on open-source software security paves the way toward technological innovation and growth, drives the rapid development of new technologies and business models, and keeps the American economy dynamic and competitive.

In 2024, the OS3I will continue to champion the security of the open-source software ecosystem by taking stock of the research and information submitted through the RFI to inform future OS3I workstreams and priority actions. Additionally, the OS3I will continue to engage Federal government, the open-source software community, civil society, and private sector stakeholders across the open-source software landscape to identify and highlight policy solutions that improve the security of the open-source software ecosystem.

---

[i] The Cybersecurity Review Board, Review of the December 2021 Log4J Event, July 11 2022 *available at*: CSRB Report on Log4j - Public Report - July 11 2022_508 Compliant (cisa.gov)

[ii] The White House, National Cyber Security, March 1, 2023 at pgs. 20-21, *available at*: National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov), *see* Strategic Objective 3.3: Shift Liability for Insecure Software Products and Services.

[iii] The White House, National Cybersecurity Strategy Implementation Plan, July 2023 at pg. 36, *available at*: National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf (whitehouse.gov).

[iv] OS3I Members include Federal staff-level representatives from: Center for Medicare and Medicaid Services (CMS), Cybersecurity and Infrastructure Security Agency (CISA), Defense Advanced Research Projects Agency (DARPA), Department of Homeland Security (DHS), General Services Administration (GSA), Lawrence Livermore National Laboratory (LLNL), National Institutes of Standards and Technology (NIST), National Science Foundation (NSF), National Security Agency (NSA), Office of the Director of National Intelligence (ODNI), Office of Management and Budget (OMB), Office of the National Cyber Director (ONCD), Office of Science & Technology Policy (OSTP), and Office of Secretary of Defense, CDAO - Defense Digital Service (DDS).

[v] Memory safety vulnerabilities [CWE-1399: Comprehensive Categorization: Memory Safety] are a class of vulnerability affecting how memory can be accessed, written, allocated, or deallocated in unintended ways in programming languages. Memory-unsafe programming languages default to allowing programmers to take actions that could result in memory safety vulnerabilities. *See* DHS CISA, The Case for Memory Safe Roadmaps, December 2023 *available at* https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf. *See also* NSA Cybersecurity Information Sheet: Software Memory Safety, November 2022 *available at* https://media.defense.gov/2022/Nov/10/2003112742/-1/-1/0/CSI_SOFTWARE_MEMORY_SAFETY.PDF.

[vi] Microsoft, MSRC Security Research, "Trends, challenge, and strategic shifts in the software vulnerability mitigation landscape" by Matt Miller, February 7, 2019 *available at*: MSRC-Security-Research/presentations/2019_02_BlueHatIL/2019_01_-_BlueHatIL_-_Trends,_challenge,_and_shifts_in_software_vulnerability_mitigation.pdf at master · microsoft/MSRC-Security-Research GitHub. *See also* The Chromium Projects, Memory Safety *available at* https://www.chromium.org/Home/chromium-security/memory-safety/.

[vii] *See generally* DHS, "CISA Open-Source Software Security Roadmap" September 2023 *available at*: https://www.cisa.gov/sites/default/files/2023-09/CISA-Open-Source-Software-Security-Roadmap-508c.pdf.