TLP:CLEAR

CISA Open Source Software Security Roadmap

September 2023

Cybersecurity and Infrastructure Security Agency

Table of Contents

Overview

The federal government, critical infrastructure, and state, local, tribal, and territorial (SLTT) governments greatly depend upon open source software (OSS). OSS is software for which the human-readable source code[1] is made available to the public for use, study, re-use, modification, enhancement, and re-distribution. OSS is part of the foundation of software used across critical infrastructure, supporting every single critical infrastructure sector and every National Critical Function: one study[2] found that 96% of studied codebases across various sectors contain open source code, and 76% of code in studied codebases was open source. Therefore, to fulfill CISA's mission of understanding, managing, and reducing risks to the federal government and critical infrastructure, we must understand and protect the open source software that we rely upon.

As a public good, open-source software is supported by diverse and wide-ranging communities—which are composed of individual maintainers, non-profit software foundations, and corporate stewards. CISA must integrate into and support these communities, with a particular focus on the critical OSS components that the federal government and critical infrastructure systems rely upon.

CISA recognizes the immense benefits of open source software, which enables software developers to work at an accelerated pace and fosters significant innovation and collaboration. With these benefits in mind, this roadmap lays out how CISA will help enable the secure usage and development of OSS, both within and outside the federal government. As detailed below, the roadmap centers on 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.

Vision

Aligning with the National Cybersecurity Strategy's goal of a "more resilient, equitable, and defensible cyberspace," CISA envisions a prosperous future where secure, resilient technology is the backbone of our world. Open source software, fostering significant growth as part of the foundation on which technology is built, is key to this future. We envision a world in which every critical OSS project is not only secure but sustainable and resilient, supported by a healthy, diverse, and vibrant community. In this world, OSS developers are empowered to make their software as secure as possible. Further, the incredible growth fostered by OSS is coupled with action from those who capitalize on OSS to be good stewards of the projects they depend on. In this world, OSS consumers responsibly use it, contributing back to the extent they can to the community and code they depend on. Similarly, consumers and integrators of these OSS projects are given the tools to ensure the packages they use are secure and well curated.

To achieve such a future, the federal government must take strong action towards maintaining and

[1] Source code is the human-readable formal language that software developers use to specify the actions a computer will take.
[2] Synopsys. "2023 Open Source Security and Risk Analysis Report." Last modified April 2023. https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

securing OSS infrastructure as reflected in the National Cybersecurity Strategy. CISA, given its responsibilities to defend and secure federal government information systems and coordinate a national effort to secure and protect against critical infrastructure risks, has a key role to play in OSS security, grounded in partnership with federal agencies, OSS consumers, and the OSS community.

Threat Model

In order to secure OSS, we must understand the relevant attacks and vulnerabilities. CISA is broadly concerned about two distinct classes of OSS vulnerabilities and attacks:

1. **The cascading effects of vulnerabilities in widely used OSS.**

As evidenced by the Log4Shell vulnerability, the ubiquity of OSS can cause vulnerabilities to have particularly widespread consequences. Given the prevalence of OSS across the federal government and critical infrastructure, any widespread vulnerability represents risk that CISA should seek to reduce. Similar to the potentially large impact of vulnerabilities in widely used closed-source software, the widespread and distributed nature of OSS can magnify the impact of OSS vulnerabilities. Hence, CISA should contribute to reducing the prevalence of exploitable vulnerabilities and aiding in response when vulnerabilities occur.

2. **Supply-chain attacks on open source repositories leading to compromise of downstream software.**

The second category of risks is the malicious compromise of OSS components, leading to downstream compromises. Examples include an attacker compromising a developer's account and committing malicious code, or a developer intentionally inserting a backdoor into their package. Real-world examples include embedding cryptominers[3] in open source packages, modifying source code with protestware[4] that deletes a user's files, and employing typosquatting[5] attacks that take advantage of developer errors.[6]

Strategic Alignment

This OSS roadmap aligns to the National Cybersecurity Strategy, including Strategic Objective 4.1, which states that the federal government will "develop and drive adoption of solutions that will improve the security of the Internet ecosystem," and Strategic Objective 3.3, which states that the federal government will collaborate with the private sector and OSS community to "invest in the development of secure software, including memory-safe languages." CISA's work in this roadmap is in

[3] Gershon, Aviad and Folkman, Tal. "'CuteBoi' Detected Preparing a Large-Scale Crypto Mining Campaign on NPM Users." Checkmarx Blog. July 6, 2022. https://checkmarx.com/blog/cuteboi-detected-preparing-a-large-scale-crypto-mining-campaign-on-npm-users/.
[4] Trend Micro Research. "How Shady Code Commits Compromise the Security of the Open-Source Ecosystem." Trend Micro Blog. July 11, 2022. https://www.trendmicro.com/en_us/research/22/g/how-shady-code-commits-compromise-the-security-of-the-open-sourc.html.
[5] Tal, Liran. "What is typosquatting and how typosquatting attacks are responsible for malicious modules in npm." Snyk Blog. January 12, 2021. https://snyk.io/blog/typosquatting-attacks/.
[6] These types of OSS supply chain attacks are described in more detail in Ladisa et al. See Ladisa, P., Plate, H., Martinez, M., and O. Barais. 2023. SoK: Taxonomy of Attacks on Open Source Software Supply Chains. Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, pp. 167-184. doi: 10.1109/SP46215.2023.00010.

fulfillment of Initiative 4.1.2 of the National Cybersecurity Strategy Implementation Plan, to "Promote open-source software security and the adoption of memory safe programming languages" via the Open Source Software Security Initiative (OS3I).

This roadmap also advances Objective 1.4 of the CISA Strategic Plan for 2023-2025, which aims to achieve a cyberspace ecosystem that is secure-by-design and secure-by-default, and helps achieve priority areas addressed through the OS3I interagency working group convened by the Office of the National Cyber Director, which include memory safety, Common Vulnerabilities and Exposures (CVE) reform, and education.

Lastly, this roadmap aims to align, where possible, to existing OSS community efforts. Objective 1.1 below specifically speaks to integrating into community initiatives to further align CISA and OSS community work.

FY24-26 Open Source Goals & Objectives

Goal 1: Establish CISA's Role in Supporting the Security of OSS

It is crucial that CISA matures its working relationship with the OSS community to build a secure and resilient open source ecosystem. In line with CISA's mission, this means identifying and reducing risks to the federal government and critical infrastructure and contributing back to help improve the security of the broader OSS ecosystem.

To achieve this, CISA must have the capabilities to understand the OSS ecosystem and collaborate with the OSS community. CISA recognizes that the open source community is not starting from scratch and already has many initiatives underway focused on security. CISA strives to align with and amplify these initiatives with the goal of channeling the federal government's authorities and capabilities to foster greater OSS security.

Objective 1.1. Partner With OSS Communities

CISA will show up as an OSS community member, working hand-in-hand with OSS communities. Similar to how CISA has formed partnership groups with companies across various sectors, CISA will establish partnerships with OSS communities. CISA will establish a real-time collaboration channel with OSS community members (including OSS foundations and community organizations, code hosting services, and package managers). This channel will allow the OSS community members to provide individual input on actions CISA is taking, individually participate in roadmap planning sessions, and allow CISA to identify additional ways to support OSS community efforts. CISA will also contribute to broader community efforts that work to strengthen the security and resiliency of the OSS ecosystem by participating in relevant community working groups on OSS security.

In addition, CISA will continue its ongoing collaborative planning effort with industry, OSS communities, and interagency partners to better understand the role OSS components currently play in industrial control system (ICS) products and develop a plan to improve those components' maintenance and security.

Objective 1.2. Encourage Collective Action From Centralized OSS Entities

Recognizing that centralized OSS entities such as package managers and code hosting services can help drive systemic security improvements, CISA will encourage collective action from and greater

accountability by these entities. CISA will participate in relevant working groups on securing these centralized entities, with the goal of working collaboratively to develop security principles for package managers and other centralized platforms in the OSS ecosystem.

Objective 1.3. Expand Engagement and Collaboration With International Partners

OSS is a public good, providing benefits for governments and private sector organizations around the world. This makes it crucial for the federal government to engage with its international partners and allies to bolster OSS security and resilience. In coordination with interagency partners, CISA will conduct engagements with international partners and allies and identify opportunities to collaborate on areas of shared interest, including the adoption of practices laid out in this roadmap.

Objective 1.4. Establish and Organize CISA's OSS Work

CISA must be organizationally structured to execute on the open source efforts described in this roadmap. To that end, CISA will increase our breadth and depth of OSS security expertise and will establish an internal CISA Open Source Software Security Working Group to coordinate CISA's work on OSS security.

Goal 2: Drive Visibility into OSS Usage and Risks

To understand where CISA can best support the security of the OSS ecosystem, we must understand where the greatest dependencies lie for the federal government and critical infrastructure. To that end, CISA will identify the OSS libraries that are most used to support critical functions across the federal government and critical infrastructure. CISA will utilize this information to understand where the greatest risks lie and prioritize activities to mitigate and reduce these risks.

Objective 2.1. Understand OSS Software Prevalence

CISA will develop a capability for assessing OSS software prevalence in the federal government and will engage federal and critical infrastructure partners to improve CISA's awareness of OSS software prevalence in critical infrastructure. For the federal government, this will involve aggregating readily available data on software prevalence from existing data sources, such as CISA's Continuous Diagnostics and Mitigation (CDM) program. For areas where data is not as readily available, such as operational technology (OT) and ICS, CISA will work to advance our capability for assessing software prevalence and underlying OSS components. The goal is to understand all software prevalence including prevalence of software that is end-of-life, end-of-support, various versions, OSS, as well as unique software that may require additional resources to secure and maintain. For critical infrastructure, CISA will work with Sector Risk Management Agencies and critical infrastructure owners and operators to identify opportunities for voluntary sharing of data.

Objective 2.2. Develop a Framework for OSS Risk Prioritization

CISA will develop a framework to conduct a risk prioritization of OSS components discovered in Objective 2.1. The framework will recommend importance criteria and prioritization factors, such as an OSS component's level of usage, level of maintenance, build process security, and code security properties—like memory safety and. The framework will leverage existing work where possible and will be released to the public.

The framework will identify various categorizations of OSS components, such as components that:

- Due to their level of usage and existing support, the federal government should directly support.
- Are malicious, which the federal government should stop using; or
- Are well supported and the government may continue using.

Objective 2.3. Conduct Risk-Informed Prioritization of OSS Projects in Federal Government and Critical Infrastructure

CISA will apply the framework described above to the repositories identified in 2.1, generating a risk-informed prioritization of OSS dependencies in the federal government and, to the degree possible, critical infrastructure. This prioritization may group OSS dependencies into various categories, as described in Objective 2.2. CISA will use this list to ensure that the federal government's OSS efforts focus on the most critical and relevant OSS dependencies. Additionally, CISA will leverage this prevalence list to further understand vulnerabilities present in OSS used by the federal government and critical infrastructure.

Objective 2.4. Understand Threats to Critical OSS Dependencies

CISA will develop a process to continuously assess threats to critical OSS dependencies, including, when available, the prioritized list of OSS dependencies generated in 2.3. When relevant, CISA will publish alerts about targeting of key OSS dependencies.

Goal 3: Reduce Risks to the Federal Government

This goal focuses specifically on securing the federal government's usage of OSS. Similar to companies that responsibly engage with OSS, the federal government must establish processes to manage our usage of OSS and means of contributing back to the OSS we depend upon.

Objective 3.1. Evaluate Solutions to Aid in Secure Usage of OSS

CISA will evaluate the feasibility and efficacy of offering future capabilities or services to aid federal agencies in addressing gaps around managing their OSS. Such services may include tools that integrate into the continuous integration and continuous delivery (CI/CD) process to assess OSS risks (e.g., flagging vulnerable/outdated dependencies) and tools that facilitate support back to open source dependencies.

Objective 3.2. Develop Open Source Program Office Guidance For Federal Agencies.

Open source program offices (OSPOs)[7] have emerged in industry, civil society, and academia as a way to manage an organization's OSS operations, including supporting the responsible usage of OSS and facilitating contributions back to OSS. CISA will develop open source program office (OSPO) best practice guidance for federal agencies and other entities who wish to implement OSPOs. CISA will support federal agencies who are interested in piloting OSPOs.

Objective 3.3. Drive Prioritization of Federal Actions in OSS Security

The Office of the National Cyber Director (ONCD) established the OS3I with the goal of advancing government policy and resources to foster greater OSS security. Working with ONCD and government

[7] TODO (OSPO) Group. "Open Source Program Office (OSPO) Definition and Guide." May 31, 2023. https://github.com/todogroup/ospodefinition.org.

partners, CISA will continue to contribute to OS3I to identify policies and resources that can be utilized to bolster OSS security and resilience.

CISA, through OS3I, will drive prioritization of federal actions that promote security and resilience within the OSS ecosystem. CISA, ONCD, the National Science Foundation (NSF), the Defense Advanced Research Projects Agency (DARPA), and the Office of Management and Budget (OMB) initiated this effort by publishing a Request for Information (RFI) on open-source software security and memory safe programming languages. Following the RFI, the authoring agencies will work to publish a report summarizing responses and identifying key areas for government action.

Goal 4: Harden the OSS Ecosystem

Recognizing the public-good nature of OSS and that any efforts to secure the broader OSS ecosystem will increase the security and resilience of the federal government and critical infrastructure, CISA will advance efforts to harden the broader OSS ecosystem. This effort will focus on OSS components identified in Goal 2 as being particularly critical for the federal government and critical infrastructure.

Objective 4.1. Continue to Advance SBOM Within OSS Supply Chains

Although the value of software bill of materials (SBOM) is broader than OSS, there are unique challenges to achieving comprehensive SBOM generation throughout open source supply chains. In addition to continuing its work to drive SBOM standardization, CISA will also focus on the requirements, challenges, and opportunities of automatically generating dependency data within the open source ecosystem. The broader SBOM work will continue to engage with the OSS community and CISA will propose collaborations as appropriate with stakeholders identified in the initiatives above.

Objective 4.2. Foster Security Education for Open Source Developers

In coordination with relevant federal agencies, including the NSF, CISA will support security education for current and future open source developers. As part of this effort, CISA, consulting with the open source community, will publish open source security toolkits that collect best practices and resources for open source security. This will include a toolkit for OSS maintainers with resources on secure software development and vulnerability disclosure,

Objective 4.3. Publish Guidance on OSS Security Usage Best Practices

CISA will publish best practices on securely incorporating OSS for entities including federal agencies, critical infrastructure organizations, and SLTT. This will include guidance for open source consumers on how to responsibly use OSS, as well as resources to understand OSS basics, a description of how OSS contributes to critical infrastructure, and OSS security basics.

Objective 4.4. Foster OSS Vulnerability Disclosure and Response

CISA will continue to coordinate vulnerability disclosure and response for OSS vulnerabilities by leveraging relationships with the OSS community. This coordination may include establishing processes to specifically look for upstream issues in open source packages that critical infrastructure organizations depend on and quickly notify affected users of the identified vulnerabilities.