IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 9, September 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Chain of Trust: A Review of Actions Taken by Industry and Government against Software Supply Chain Attacks

Varadharaj Varadhan Krishnan

Independent Researcher, Washington, USA

ABSTRACT: In the last decade, software supply chain attacks have soared in occurrence, sophistication, and size of impact. These attacks are now more common and have a widespread impact, unlike a targeted attack aimed to compromise a particular entity. Incidents like the SolarWinds and Log4j attacks really showed the breadth of impact that a compromise of a commonly used software package can have. With the increase in software supply chain attacks and its potential to cause great financial losses for private sectors and possibly affect national security, various countries across the globe have undertaken measures to address this trend. In this paper, a comprehensive review of the responses from various governments and private entities to defend against software supply chain attacks is performed. By reviewing the actions taken by different entities, the paper aims to create threat awareness and best practices to be adopted. It also brings visibility to the regulatory requirements, which is essential for maintaining compliance and avoiding legal penalties. The paper also identifies outstanding challenges and limitations that exist today with respect to defending against software supply chain attacks; by identifying and presenting these, this paper paves the way for future work to address these limitations and challenges.

KEYWORDS: Software Supply Chain Attack, Cybersecurity, Government Response, Cyber defense, Cybersecurity Framework.

I. INTRODUCTION

A software supply chain attack can be described as a cyber-attack where the threat actor infiltrates a software vendor's network and deploys malicious code to compromise the vendor's software product before it is distributed to their customers. The compromised software is then used by the threat actor to compromise the customer's network and data systems. A supply chain attack may involve new software that may be compromised from the beginning or a compromise through other incremental updates like a patch or hotfix. This kind of supply chain attack affects all users of the compromised software and can have widespread consequences for the government, critical infrastructure operators, and private sector software companies [1]. A compromised software supply chain can have profound consequences; even a minor vulnerability can lead to devastating breaches and significant impact because of the number of entities falling victim to one attack. Most modern software today isn't developed from scratch; most often, it is a mashup and combination of various software artifacts containing open-source software, and at the same time, all organizations use a variety of software from various vendors. Software used or produced by an organization has a significant dependency on software components not created by the organization. These external dependencies do have their own vulnerabilities, and developers have no control over the source code from the third party; developers often might not use the software packages with the latest updates or consistently update all the packages. Cyberattacks like the one against SolarWinds and its customers and exploits that took advantage of vulnerabilities in open-source software like Log4j highlight weaknesses within the software supply chain, an issue that spans both commercial and open-source software and impacts both private and government organizations [2]. Today, there is an increased demand for software supply chain security awareness. In this paper, we will discuss the software supply chain risks and attacks and how various governments and private entities have responded to the rise in software supply chain attacks. The paper's objective is to review these response measures and their impact and serve as input for private and public organizations looking to step up their efforts against software supply chain attacks.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. BACKGROUND

Supply chain attacks generally have severe consequences for organizations, their client base, and sometimes entire industries. Organizations falling victim to supply chain attacks often endure considerable financial losses due to loss of service, lost opportunity for revenue generation, and significant costs associated with attack remediation [1]. Furthermore, companies also suffer from reputational damage, which can eventually lead to the loss of their customers. Successful supply chain attacks can result in data breaches and loss of customer PII and intellectual property. Again, the impact of data breaches is not restricted to the company; instead, it affects the clients who trust them with their valuable digital assets and customer data. Rebuilding trust will be challenging and lead to long-term losses, including the loss of a customer [2]. Supply-chain attacks targeted at critical infrastructure like defense systems, public water supplies, energy generation and distribution sites, and transit systems pose a great threat to national security. These attacks can disrupt basic and essential services and can directly impact large populations of a country. Lastly, organizations impacted by supply chain attacks can experience regulatory fines if they fail to comply with data protection laws such as the GDPR or CCPA. In the past, software supply chain breaches were rare and rare. They were also usually executed by sophisticated attackers. One of the most notable supply chain breaches in recent years was the SolarWinds attack, which was attributed to the Russian APT group named APT29 [2]. But in the last three years, almost two-thirds (61%) of U.S [17]. Businesses were affected by such an attack, with at least one of their key suppliers being hacked. These attacks have become a common and serious issue for organizations and businesses all around the world. The barrier for a successful software supply chain attack was further lowered in 2024 and has increased throughout 2023 and 2024 [18]. They are found across various popular open-source projects, most notably npm and PyPI. Now, the landscape of supply chain attacks has broadened, and sophisticated nation-state actors and less resourceful beginner threat actors can perform such attacks through open-source projects.

III. GOVERNMENT ACTIONS

A. UNITED STATES

The United States has taken many strong proactive measures to address the fast-escalating trend of software supply chain attacks. The US government has a deep understanding of the emerging issue and how it can pose a threat to national security and possibly undermine economic stability.

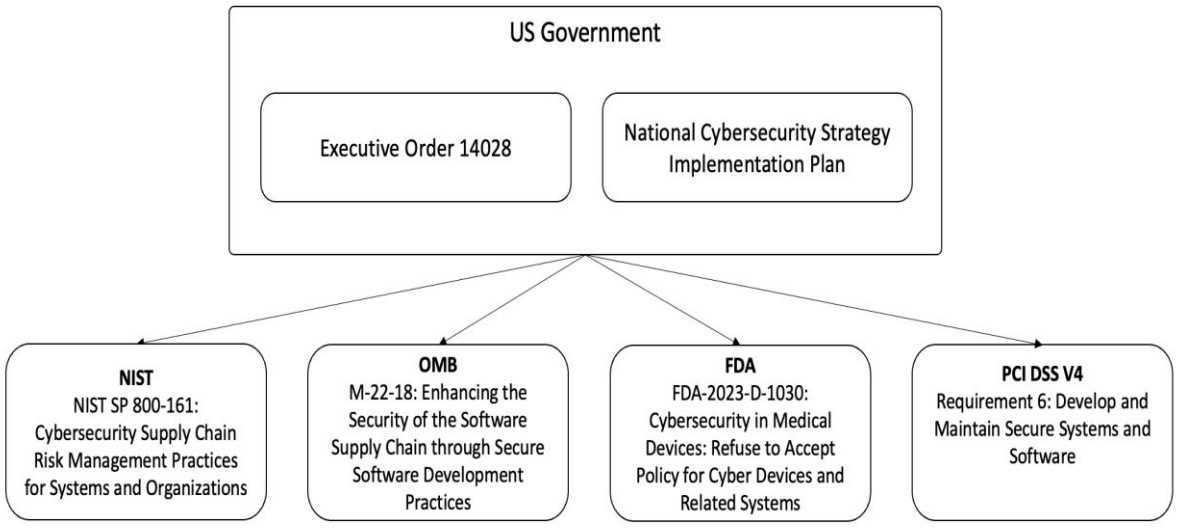

Figure 1. US Government initiatives against software supply chain attacks

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A1.National Cybersecurity Strategy

The 2023 National Cybersecurity Strategy (NCS) set a comprehensive framework for creating a resilient digital ecosystem [3]. The strategy emphasized the importance of cybersecurity for national security. It recognized that a secure digital ecosystem is essential for all Americans and called for collaboration between the public and private sectors. Another critical aspect of the strategy is shifting the responsibility of cybersecurity away from end-users to private and public entities that are in the best position to manage risk and defend meaningfully against threat actions. The strategy called for investments to establish long-term cybersecurity resilience. The NCS has five pillars: i. Defend critical infrastructure, ii. Disrupt and dismantle threat actors, iii. Shape market forces to drive security and resilience, iv. Drive investments in a resilient future, and v. Forge international partnerships to pursue shared goals. The strategy also includes specific objectives like holding organizations accountable for data security, limiting the collection and use of sensitive personal data, and holding organizations liable for software vulnerabilities. NCS further laid out investment objectives, improving infrastructure cybersecurity through federal grants, prioritizing cybersecurity research and development, and leveraging federal procurement to enhance accountability [3]

A2. Executive Order on Improving the Nation's Cybersecurity

The U.S. government has introduced several legislative and regulatory measures to improve the security posture of the software supply chain. One of the most significant actions was Executive Order 14028, issued in May, 2021titled "Executive Order on Improving the Nation's Cybersecurity." [4] With this EO, the US government mandated a stringent cybersecurity standard for software used by federal agencies. One of the main technical requirements set by the US government was a mandate for federal suppliers to provide a Software Bill of Materials (SBOM). A Software Bill of Material (SBOM) is a comprehensive inventory of components that comprise an application or a software product. SBOM is supposed to include open-source and commercial third-party libraries, API calls, versions, and licenses.

A3. Federal Agency Initiatives

The US government's key federal agencies, like the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA), have played a significant role in implementing various cybersecurity initiatives. CISA, in collaboration with the NSA, released comprehensive guidelines for securing the software supply chain. These guidelines include best practices for managing open-source software, implementing SBOMs, and ensuring the integrity of software throughout its lifecycle [5][6]

A4. Enduring Security Framework

It is important to have collaboration between the public and private sectors in the fight against software supply chain attacks. The U.S. government has incubated multiple collaboration initiatives to enhance information sharing, improve threat intelligence, and develop coordinated responses to supply chain attacks. One of them is the Enduring Security Framework (ESF) [7]. The Enduring Security Framework (ESF) is a public-private partnership that aims to address risks to critical infrastructure and National Security Systems. ESF is a cross-sector working group that operates under the guidance of the Critical Infrastructure Partnership Advisory Council (CIPAC) to address threats and risks to the security and stability of U.S. National Security Systems and critical infrastructure. ESF is chartered by the Department of Defense, Department of Homeland Security, Office of the Director of National Intelligence, and the IT, Communications, and Defense Industrial Base Sector Coordinating Councils [7].

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

B. EUROPEAN UNION

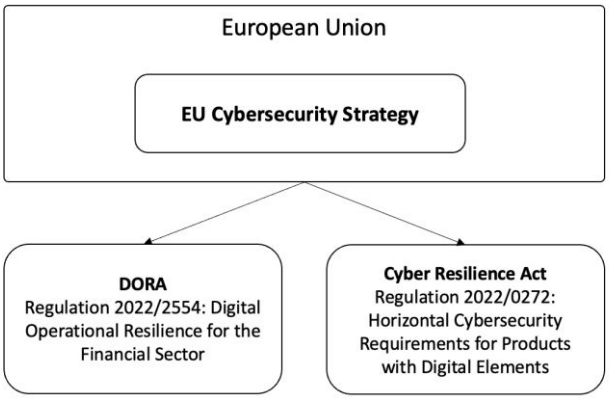

Figure 2 European Union Initiatives Against Software Supply Chain Attack

B1. CYBER RESILIENCE ACT

The European Cyber Resilience Act (CRA) [8] established a set of rules that aimed to improve the cybersecurity of digital products and services. The CRA applies to all the supply chains of digital products, including manufacturers, distributors, and importers, respecting the geographical location of the organization or the location where the product was developed. The CRA entered into force on March 12, 2024 [8].

The key mandate of CRA regarding software supply chain security is that it mandates products to meet cybersecurity requirements at every stage of the development and maintenance process, including automatic security updates. Companies also need to conduct cyber risk assessments before a product is put on the market and throughout ten years of its expected lifecycle. Companies would have to notify the EU cybersecurity agency ENISA of any incidents within 24 hours of becoming aware of them and take measures to resolve them. ENISA ('European Union Agency for Cybersecurity') is an agency that provides support to EU member states, businesses, and institutions in the cybersecurity sector and delivers solutions and improvements to the EU's cybersecurity framework. Its role is to promote and support member states, businesses, and EU institutions in dealing with cyber-attacks.

The CRA also required products to display a CE marking to indicate that they are compliant with the new standard. Non-compliance with the CRA will result in significant fines, up to €15 million or 2.5% of a company's global turnover. The main purpose of CRA is to improve consumer trust and safety.

B2. EU DIGITAL OPERATION RESILIENCE FOR THE FINANCIAL SECTOR (REGULATION 2022/2554)

The EU Digital Operational Resilience Act (DORA) incorporates several provisions addressing supply chain transparency, risk assessments, and information security responsibilities between entities producing digital products and services and their consumers. This is done through very prescriptive stipulations and oversight processes [9]. DORA requires entities to institute secure software development methodologies vetting systems through the entire lifecycle via extensive testing upholding best practices like OWASP standards, mitigating risks from flawed architectures, protocols, or source code vulnerabilities that external threat actors can exploit (EU DORA, 2022) [9]. DORA also requires financial entities to undertake due diligence assessments on potential third-party technology/service providers, examining aspects like security track record, breach histories, redundancy capacities, and overall cyber maturity through audits and attestations before partnerships.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

B3. ENISA CYBERSECURITY CERTIFICATION FRAMEWORK

ENISA's cybersecurity certification program aims to provide criteria for carrying out security assessments to determine the compliance level for digital products and services against specific requirements. Cybersecurity certification requires the formal evaluation of products, services, and processes by an independent and accredited body against a defined set of criteria and standards and the issuing of a certificate indicating conformance. As such, cybersecurity certification plays a key role in increasing trust and security in products, services, and processes [10].

C. UNITED KINGDOM

C1. NATIONAL CYBER SECURITY CENTRE (NCSC) GUIDELINES AND PROPOSALS

UK's National Cyber Security Centre has specific guidelines published for software supply chain security. The guidance was aimed to provide organizations with an improved awareness of supply chain security and the adoption of good practices to defend against supply chain attacks. The guidance proposed 12 principles designed to establish effective control and oversight of an organization's supply chain. These principles can be broadly classified into four categories. i. Understand the risks, ii. Establish control iii. Check your arrangements, and iv. Continuous improvements. [11]

D. OTHER COUNTRIES

D1. AUSTRALIAN – INFORMATION SECURITY MANUAL (ISM)

In March 2024, the Australian Signals Directorate published the latest update to its Information Security Manual (ISM). The ISM provides a framework based on risk management principles and best practices to help cyber security professionals protect their systems and data from cyber threats. The ISM includes cyber security guidelines designed to 'provide practical guidance on how an organization can protect its systems and data from cyber threats.' The ISM is a framework; organizations are not yet required by law to comply.

Regarding software supply chain security, ISM control ISM-1730 states that producers of digital products should provide a software bill of material to the software consumers [12]. Control ISM-1616 states that the software producer should establish a vulnerability disclosure program. These two controls established in the guideline play an important role in strengthening our defenses against software supply chain attacks.

IV. INDUSTRY ACTIONS

A. OPEN-SOURCE SECURITY INITIATIVES

A1. ROLE OF THE OPEN-SOURCE SECURITY FOUNDATION (OPENSSF)

The Open-Source Security Foundation (OpenSSF) is a community of software developers and security engineers who work together to improve the security of open-source software (OSS) for the public good. OpenSSF is a cross-industry initiative that's part of the Linux Foundation and brings together open-source security initiatives and their supporters. After the Log4j incident [], OpenSSF launched the Alpha-Omega Project.

Alpha Omega Project [13]: During the aftermath of the Log4j incident, OpenSSF met with government and industry leaders at the White House and announced the Alpha-Omega Project to improve the security posture of open-source software (OSS) through direct engagement of software security experts and automated security testing. Microsoft and Google pledged to support the Alpha-Omega Project with an initial investment of $5 million. Widely deployed OSS projects that are critical to global infrastructure and innovation have become top targets for adversarial attacks. Adversaries are quick to react to the disclosure of vulnerabilities in OSS software, and within hours, attacks start to appear. The Alpha-Omega Project's goal is to improve global OSS supply chain security by working with project maintainers to systematically look for new, as-yet-undiscovered vulnerabilities in open-source code and get them fixed. "Alpha" will work with the maintainers of the most critical open-source projects to help them identify and fix security vulnerabilities and improve their security posture. "Omega" will identify at least 10,000 widely deployed OSS projects

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

where it can apply automated security analysis, scoring, and remediation guidance to their open-source maintainer communities [13].

Protobom [14]: OpenSSF, in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), launched Protobom, a new and innovative open-source software supply chain tool. Protobom enables all organizations, including system administrators and software development communities, to read and generate Software Bill of Materials (SBOMs) and file data, as well as translate this data across standard industry SBOM formats. SBOMs are key to strengthening software security and software supply chain risk management. Understanding the software supply chain, obtaining an SBOM, and using it to analyze known vulnerabilities is crucial for managing cybersecurity risk. Currently, multiple SBOM data formats and identification schemes exist in the industry, which makes it challenging for organizations wanting to adopt SBOM usage. Protobom aims to mitigate this issue by offering a format-neutral data layer on top of the standards that let applications work seamlessly with any kind of SBOM [14]

A2. INTRODUCTION OF FRAMEWORKS LIKE SLSA AND S2C2F

Supply-chain Levels for Software Artifact (SLSA) [15] is a set of incrementally adoptable guidelines for supply chain security established by industry consensus. The specifications set by SLSA are useful for both software producers and consumers: producers can follow SLSA's guidelines to make their software supply chain more secure, and consumers can use SLSA to make decisions about whether to trust a software package. SLSA offers [15]:

- A common vocabulary to talk about software supply chain security
- A way to secure your incoming supply chain by evaluating the trustworthiness of the artifacts you consume
- An actionable checklist to improve your own software's security
- A way to measure your efforts toward compliance with forthcoming Executive Order standards in the Secure Software Development Framework (SSDF)

Secure Supply Chain Consumption Framework (S2C2F) Project [16]: The S2C2F was built and donated by Microsoft, where it has been used and refined internally since 2019. It was built as a consumption-focused framework that uses a threat-based, risk-reduction approach to mitigate real-world threats. The framework enumerates a list of real-world supply chain threats to OSS and explains how the framework's requirements mitigate those threats. The requirements are organized into four levels of maturity.

Level 1 – represents a basic set of governance practices already applied by many organizations, such as using package managers (to automate tracking and updating of reused components), inventorying your OSS, scanning for known vulnerabilities, and updating OSS dependencies.

Level 2 – builds upon Level 1 by leveraging technology that helps improve your Mean Time to Remediate (MTTR) vulnerabilities, with the goal of fixing them faster than the adversary attacks.

Level 3 – is focused on proactive security analysis combined with preventative controls that mitigate against accidental consumption of compromised or malicious OSS, problems that are much less common but can be harmful if they occur.

Level 4 – represents controls that mitigate against the most sophisticated attacks but are also the most difficult to implement at scale; therefore, level 4 should be considered aspirational in many situations and reserved for your dependencies in your most critical projects [16]

V. CHALLENGES AND LIMITATIONS

Securing software supply chains presents a wide variety of technical challenges. These challenges are further compounded by the complexity and interconnectivity of modern software development and distribution processes. Modern software is often built using layers of third-party components, open-source libraries, and APIs. This makes it difficult to maintain a detailed inventory of all dependencies and their associated vulnerabilities. The widespread use of open-source software further complicates this issue. Log4j incident was a prime example. For an organization,

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

achieving full visibility into its software supply chain is a daunting task. Typically, many organizations don't have any effective way to track the provenance and integrity of the software components used within the organization. Implementing an SBOM solution can help address these challenges, but widespread adoption of SBOM is another challenge on its own.

Effective supply chain security requires coordination among multiple stakeholders, including software developers, suppliers, and end-users. Achieving this level of collaboration is often met with resistance in the form of organizational security policies, different priorities, and resource constraints. Public-private partnerships, like the initiatives by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), aim to bridge these gaps, but the challenges continue to exist.

VI. CONCLUSION

The rise of software supply chain attacks has raised concerns for businesses and government bodies worldwide. Governments around the world have taken action to address this issue through a range of strategic measures. Through the review of the responses from various governments and private entities against supply chain attacks, the paper created threat awareness and shed light on the regulatory requirements with respect to software supply chain security, thus saving businesses and other entities from legal penalties. This study also highlights the challenges and constraints in the modern software development environment. By pinpointing and outlining these challenges, the study sets the stage for future efforts to tackle these challenges. Lastly, this paper also acts as a reference for understanding worldwide initiatives aimed at curbing software supply chain attacks.

REFERENCES

1. Defense Technical Information Center. (2020). Securing the supply chain from cyber-attack: Challenges and best practices (Report No. AD1108057). Retrieved from https://apps.dtic.mil/sti/trecms/pdf/AD1108057.pdf
2. Boyens, J., Paulsen, C., Bartol, N., Moorthy, R., & Shankles, S. (2014). Supply chain risk management practices for federal information systems and organizations (NIST Special Publication 800-161). National Institute of Standards and Technology. Retrieved from
3. White House. (2023). National cybersecurity strategy 2023. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
4. White House. (2021, May 12). Executive order on improving the nation's cybersecurity. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
5. Cybersecurity and Infrastructure Security Agency (CISA). (2023, November 9). CISA, NSA, and partners release new guidance on securing the software supply chain. Retrieved from https://www.cisa.gov/news-events/alerts/2023/11/09/cisa-nsa-and-partners-release-new-guidance-securing-software-supply-chain
6. Cybersecurity and Infrastructure Security Agency (CISA). (April 2021). Defending against software supply chain attacks. Retrieved from https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
7. National Security Agency (NSA). (n.d.). Enduring Security Framework. Retrieved from https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Enduring-Security-Framework/
8. European Commission. (n.d.). Cyber resilience act. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
9. Digital Operational Resilience Act. (n.d.). Retrieved from https://www.digital-operational-resilience-act.com/
10. European Union Agency for Cybersecurity (ENISA). (n.d.). Cybersecurity certification framework. Retrieved from https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework
11. National Cyber Security Centre (NCSC). (October 2023). Supply chain security: 12 principles infographic. Retrieved from https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-security-12-principles-infographic
12. Australian Cyber Security Centre (ACSC). (June 2024). Guidelines for software development. Retrieved from https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-software-development

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

13. Open Source Security Foundation (OpenSSF). (2022, February 1). OpenSSF announces the Alpha-Omega project to improve software supply chain security for 10,000 OSS projects. Retrieved from https://openssf.org/press-release/2022/02/01/openssf-announces-the-alpha-omega-project-to-improve-software-supply-chain-security-for-10000-oss-projects/
14. Open Source Security Foundation (OpenSSF). (2024, April 16). CISA, DHS S&T, and OpenSSF announce global launch of software supply chain open source project. Retrieved from https://openssf.org/press-release/2024/04/16/cisa-dhs-st-and-openssf-announce-global-launch-of-software-supply-chain-open-source-project/
15. Aqua Security. (October, 2022). SLSA: Supply chain levels for software artifacts. Retrieved from https://www.aquasec.com/cloud-native-academy/supply-chain-security/slsa/
16. GitHub. (2022). S2C2F: Secure supply chain consumption framework. Retrieved from https://github.com/ossf/s2c2f
17. Gartner. (2023, October). Mitigate enterprise software supply chain risks. Retrieved from https://www.gartner.com/doc/reprints?id=1-2FQVRV5F&ct=231127&st=sb&
18. Sonatype. State of the software supply chain: Modernizing open-source dependency management. Retrieved from https://www.sonatype.com/state-of-the-software-supply-chain/modernizing-open-source-dependency-management

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details