

# Software Supply Chain Resilience in 2025: A Comparative Analysis of Major Incidents Using OSINT Methodologies

Adelaida STĂNCIULESCU<sup>1</sup>, Ioan C. BACIVAROV<sup>2</sup>

<sup>1</sup> Bucharest Court, Bucharest, Romania

adelaida.stanciulescu@gmail.com

<sup>2</sup> Romanian Association for Information Security Assurance (RAISA)

ioan.bacivarov@raisa.org

## Abstract

The year 2025 marked a significant increase in software supply attacks chain, highlighting a strategic shift in the way the malicious actors operate. Unlike previous years, the 2025 incidents demonstrated a clear focus on compromising critical development infrastructures, cloud service providers, and open-source ecosystems with global impact. This article performs a comparative analysis of the main major software supply incidents chain reported in 2025, examining attack vectors, propagation mechanisms, operational impact, and implications for current software security models.

**Index terms:** software supply chain, OSINT, CI/CD compromises, open-source security, SBOM, cyber incidents 2025

## References

- [1]. CW Ten, "Software supply chain attacks: taxonomy and analysis," in *Proc. IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, 2022, pp. 112-126.
- [2]. SE Simion and R. Chinchani, "Trends in software supply chain threats," *IEEE Security & Privacy*, vol. 21, no. 3, pp. 28-37, 2024.
- [3]. Microsoft Security, "CI/CD supply chain attacks observed in 2025," 2025. Online. Available: <https://www.microsoft.com/security>.
- [4]. Google Security Team, "Build system compromise and mitigations," 2025. Online. Available: <https://security.googleblog.com>.
- [5]. J. Cappos et al., "On the security of modern software distribution," *ACM CCS*, New York, NY, USA, 2023, pp. 85-99.
- [6]. ENISA, "Threat landscape for supply chain attacks," 2025. Online. Available: <https://www.enisa.europa.eu>.
- [7]. M. Kuppinger, "Abuse of enterprise software updates," *Computers & Security*, vol. 131, pp. 103-118, 2025.
- [8]. CISA, "Software supply chain incident response guidance," 2025. Online. Available: <https://www.cisa.gov>.

- [9]. AZ Wang, "Comparative study of supply chain compromises," in *Proc. NDSS*, San Diego, CA, USA, 2024, pp. 201-215.
- [10]. NIST, *Secure Software Development Framework (SSDF)*, SP 800-218, Gaithersburg, MD, USA, 2025.
- [11]. B. Kitchenham et al., "Governance challenges in secure software supply chains," *IEEE Software*, vol. 41, no. 1, pp. 52-60, 2025.
- [12]. ISO/IEC 27005, *Information technology - Security techniques - Information security risk management*, International Organization for Standardization, 2018.
- [13]. MITRE, *Common Vulnerabilities and Exposures (CVE) and CVSS v3.1 Specification*, MITRE Corporation, 2019.