SYNOPSYS®

WHITE PAPER

Supply Chain Resiliency

Executive summary

In response to current events, many customers have reached out to Synopsys with questions about managing risk related to vulnerabilities in software, services, or hardware sourced from their vendors. This aspect of securing your infrastructure affects many, if not all, of the domains in cyber security—from legal and governance frameworks to advanced threat detection.

This paper is meant to serve as a reference for customers, to both frame potential risks and outline how Synopsys can help achieve the goals of supply chain security through tools, testing, and/or professional services.

Individual needs will vary depending on your firm, and your actions should be tailored to your environment, risk profile, and the unique characteristics of your organization. Our overall recommendations for consumers and producers are outlined below.

Consumers

For organizations that are end users of a cyber product, the immediate need is to detect the presence of potential breaches. This is particularly important if your organization has been directly impacted by recent attacks. Next, engage in a risk discovery and framing exercise, following frameworks outlined by international standards bodies. These activities can include:

- Discovering potentially high-risk systems
- Evaluating the vendor(s) of those systems' security programs
- Conducting risk assessments on the individual deployments of those systems
- Developing vendor requirements based on industry guidance
- Developing technical, legal, and governance controls based on analysis findings
- Working with vendors to verify attestation and maturity evolution in supply chain security requirements

Producers

For organizations that supply cyber products to consumers, the immediate need is to investigate individual codebases to ensure that no unintended functionality has been included in current builds or deployments. Then, a similar path of risk management and framing exercise should occur in accordance with standard frameworks outlined by international standards bodies and industry leaders. These activities can include:

- Discovering potentially high-risk systems with attractive functional profiles
- Conducting vulnerability and risk management evaluations on development pipelines
- Developing technical and organizational controls to address risk
- Conducting an evaluation of the software development life cycle (SDLC) consistent with reducing the potential for vulnerable or compromised code
- Conducting risk management activities on system delivery and/or deployment frameworks
- Developing additional controls in response to discovered risks
- Managing vendor risk for integrated third-party components

Overall, your efforts should focus on two basic questions related to strategic and tactical goals:

- Am I the victim of a current attack?
- How do I mitigate the risk of a supply chain attack?

Background

In December 2020, it was revealed that malicious code inserted into the SolarWinds Orion platform had compromised the supply chains of many large organizations and government agencies. This code was introduced into the build environment and deployed by a standard release cycle as part of updates to SolarWinds customer installations. The malicious code was then used as a high-privilege pivot point into internal networks where additional post-exploitation efforts were executed. Because SolarWinds Orion is a collection of modules that primarily carry high-privilege service accounts to monitor systems and collect data, it was a valuable asset for cyber criminals to use in targeting other networks.

This paper is not intended to be a reference for details of the attack. The techniques, tools, and processes (TTPs) used by the attackers are still evolving at the time of this writing, with major revelations coming as recently as mid-January 2021. These TTPs are not necessarily new; however, they were crafted with diligence, intent, and possibly insider knowledge of SolarWinds processes and pipeline.

For up-to-date information on the attack itself, please consult the following resources:

- FireEye
- CrowdStrike
- SolarWinds
- CISA

Some key takeaways from current analysis (January 26, 2021) include:

- Multiple vulnerabilities in SolarWinds' own infrastructure led to build pipeline compromise
- The attacker likely had detailed knowledge of the tools and processes used in the SolarWinds environment
- Care was taken to avoid triggering or removing build tool alerts and warnings
- Malware was deployed as part of a signed update
- Similar common weaknesses in typical information security blocking and tackling at victim sites were exploited to avoid detection

The bottom line: There is no preventative or detective control domain within the cyber security realm that is unaffected by this attack, ranging from legal frameworks to advanced threat detection.

Generic attack taxonomy

Threats to the cyber supply chain are not new. The generic attack taxonomy typically involves:

1. Attacker injects unintended functionality during development or deployment stages
2. Vendor deploys malicious functionality with legitimate product or delivery method
3. Customer receives, deploys, or updates their systems with affected code
4. Post-exploitation effort by threat agent occurs

Previous examples (anonymous and publicly published) of these attack types include:

- Malicious product updates
  - Havex remote access trojan
  - Stuxnet
- Software with malicious code inserted
  - CCleaner (twice)
  - MeDoc financial software (Ukraine)
- Development tools
  - XcodeGhost
  - GitHub and other repository typosquatting or malicious libraries

These attacks range from tampered hardware to compromised enterprise software, similar to the SolarWinds example. Attacks can also include exploiting software download portals or professional services tools to serve malicious content (similar result as Step 3 above but addressing Step 2 post-development).

Synopsys has published several blog posts and reports on the topic of supply chain risks and security. Here are three useful references:

- White paper
- Analyst report
- Blog post

How can Synopsys help?

The core capability and objective of the Synopsys Software Integrity Group is to assist customers in discovering, understanding, and mitigating risks through a combination of tools, testing, and professional services. This includes reducing the ability of an attacker to leverage vulnerabilities in provided (third-party) and deployed applications.

Secure development and code quality tools

Synopsys tools help address a wide range of security and quality defects while integrating seamlessly into DevOps environments. Our tools identify bugs and security risks in proprietary source code, third-party binaries, and open source dependencies, as well as runtime vulnerabilities in applications, APIs, protocols, and containers.

Our tools can be deployed based on individual environment and technology needs.

Penetration testing

Synopsys penetration testing services help customers understand risks to infrastructure, systems, and individual products, such as:

- Development environments and tools
- A specific system of interest
- Individual applications, including third-party developed software
- Individual products, including hardware and Internet of Things (IoT) environments

Consulting services

Synopsys professional services help many customers achieve their key goals around supply chain security. They include, but are not limited to:

Malicious code detection

Synopsys uses a combination of automated tooling and professional analysts to investigate codebases for potentially malicious code. Because much malicious code acts and looks like a normal function, a tools-directed human analysis activity helps ensure code is free from unintended functionality.

SDLC evaluations

Our team has several evaluations, assessments, and process analysis services to ensure security rigor across the development life cycle—from initial design and concept risk assessments to cloud deployment.

These evaluations help you understand what activities, practices, and procedures to include in your SDLC to address the security of implemented code.

Vendor or supply chain risk management

Synopsys leverages our expertise in assessing development processes and technical controls in the SDLC to help organizations that develop systems apply the same principles to assess their vendors. The evaluations listed above can be used to illuminate where your vendors are in their overall security maturity efforts and assist in driving mitigation controls and governance frameworks.

Threat modeling and architecture risk assessment

Similar to our testing services, Synopsys can evaluate various environments for architectural risks prior to any implementation testing. This allows customers to fully understand the risk potential of each environment or system in scope, which then either directs testing efforts or helps remediate issues prior to testing. (Many technical evaluations find implementation risks but overlook those that are built into the system at a more fundamental level.)

This can be done for high-risk deployments, development environments, deployment strategies, and even service processes.

Implementation consulting and training

Our industry-leading experts can assist in developing remediation plans, evolutionary maturity programs, and other tooling-related implementation guidance as required by your unique needs. This includes containerization, cloud deployments, continuous integration / continuous delivery (CI/CD) environments, DevSecOps, and more.

What should you do next?

Consumer checklist

Action	Relevant Synopsys SIG services
Ensure no active incidents are occurring	Malicious code detection (if suspect system is identified)
Assess environment for high-risk systems	• Architectural risk assessment • Threat modeling • Consulting services: Implementation consulting • Penetration testing
Engage in vendor assessment	• Building Security in Maturity Model (BSIMM) • Consulting services: Vendor and supply chain management
Evaluate vendors for program maturity and triage high risk	Consulting services: Vendor and supply chain management
Develop vendor requirements	Consulting services: Implementation consulting
Develop mitigating controls for high-risk systems	Consulting services: Implementation consulting
Evaluate risk of internally developed code	See producer checklist

Producer checklist

Action	Relevant Synopsys SIG services
Ensure no active incidents are occurring	• Malicious code detection (if suspect system is identified) • Code evaluation tools based on technology employed
Evaluate products or services with attractive functional profiles	• Architectural risk assessment • Threat modeling • Consulting services: Implementation consulting
Complete vulnerability management pass on development and deployment pipelines	• Consulting services: Implementation consulting • Penetration testing (optional) • Configuration evaluation (e.g., cloud deployment)
Complete risk assessment of development pipeline and deployment practices	• Architectural risk assessment • Threat modeling
Develop relevant controls	Consulting services: Implementation consulting
Evaluate software development life cycle (SDLC) and deployment practices for security-related gaps	• SDLC evaluations • BSIMM • CI/CD Maturity Action Plan (MAP) • DevSecOps MAP • Custom
Evaluate third parties and vendors integrated into products	See consumer checklist
Address internal environment from consumer perspective	See consumer checklist

SYNOPSYS®

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com