SYNOPSYS®

Procurement Language for Supply Chain Cyber Assurance

Procurement Language for Supply Chain Cyber Assurance

Introduction

For optimal viewing of this PDF, please view in Adobe Acrobat.

This document serves as a minimal set of requirements for any supplier providing network-connectable software, systems, or devices as part of a contractual bid to _____.

A description of the required methods by which features and functions of network-connectable devices are expected to be evaluated at the product level and tested for known vulnerabilities and software security weaknesses while also establishing a minimum set of verification activities intended to reduce the likelihood of exploitable weaknesses that could be vectors of zero-day exploits that may affect the device are articulated throughout this document. While this document serves as a minimal set of requirements, _____ expects that suppliers will remain conscious of the dynamic nature of cybersecurity and provide incremental improvements as needed, which _____ shall consider for inclusion in future versions of this document. Suppliers shall be required to provide _____ with any and all requested artifacts as evidence that the supplier is in compliance with stated requirements.

Scope

These requirements applies to (but is not limited to) the following:

- Application Software
- Embedded Software
- Firmware
- Drivers
- Middleware
- Operating Systems

The requirements in this document are derived from various industry standards, guidelines, and other documents including, but not limited to:

- IEC 62443
- ISO 27001
- NIST SP 800-53
- NIST SP 800-82
- DHS Cyber Security Procurement Language for Control Systems
- ISA EDSA
- FIPS 140-2
- Common Criteria Smartcard IC Platform Protection Profile
- Mayo Clinic Technology and Security Requirements Procurement Language
- UL 2900

The requirements in this document apply to devices, software or software services that will be referred to as “product” throughout this document. The product can be connected to a network (public or private) and may be used as part of a system. These requirements are applicable to products that contain software where unauthorized access or operation, either intentional or through misuse, of the product can impact safety, privacy, loss of data and compromise operational risks.

Glossary of Terms

Robustness Test Tool – specialized test tool that performs both Resource Exhaustion Tests and Invalid messages tests.

Data Resource Exhaustion Tests – Tests that try to exhaust a particular data handling resource of the product. An example is a test that tries to create as many concurrent TCP connections as possible.

Invalid Messages Tests – Tests that send incorrect data messages to the product. These messages are incorrectly structured in that they do not conform to protocol specifications either based on the structure of the message or compliance to the protocol specification.

Known Vulnerability Scanner – specialized test tool that performs known vulnerability scans off of a published vulnerability database

Known Vulnerability – vulnerability is an undocumented feature or defect which allows an outside entity to compromise the intended use and function of the product. A known vulnerability has been publicly disclosed and is typically present on a public database, such as the NIST National Vulnerability Database.

Malware – hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

Communication Protocol Fuzz Testing – the ability to transmit valid and invalid messages to the product. This allows the ability to test the product to identify any vulnerabilities that are unknown that can be uncovered by malformed inputs to the product.

Static Analysis – a process where a program's source code or its binary code is analyzed without executing the code.

Static code analysis has the ability to examine and process source code files for security weaknesses and to identify potential vulnerabilities.

Static binary analysis has the ability to examine and process compiled binaries for software components and known vulnerabilities in those components.

Common Vulnerabilities and Exposures (CVE™) – CVEs common names and identifiers for publicly know information security vulnerabilities

Common Weakness Enumerations (CWE™) – CWEs are defined software weaknesses related to architecture and design of the software.

Binary Code – defines machine instructions for a specific family of processor architecture

Byte Code – instructions that are created from source code as an intermediate step before generating machine instructions. Byte code is independent of specific processor architecture.

Dynamic Runtime Analysis – is the ability to examining the how the software behaves while it is executing or in operation.

Penetration Testing – is a mechanism of evaluation of a product, system, network or organization to identify vulnerabilities and security flaws and possibly exploit the flaws and vulnerabilities with the intent to penetrate the product, system, network and/or organization security. The intent is to circumvent or defeat the security measures of the product. Penetration testing is a largely undefined field of study that requires specialized skills found in penetration testing professionals.

Supplier – The organization supplying a product or service to _____.

Code Signing – The process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed by use of a cryptographic hash.

Requirements

The requirements section of this document will be broken out into the following sections:

1. Product Development Specification and Policy

2. Security Program

3. System Protection and Access Control

4. Product Testing and Verification

5. Deployment and Maintenance

The word "shall" precedes all requirements to indicate that they are normative. The word "Note:" precedes statements that are explanatory or informative.

1. Product Development Specification and Policy

Supplier shall represent and warrants that it has established and implements security standards and processes that must be adhered to during all equipment and product development activities, with such security standards being designed to address potential security incidents, product vulnerability to unauthorized access, loss of functions, malware intrusion, or any other compromise to confidentiality, integrity, or availability. Supplier shall represent that its security standards practices contain include testing procedures and tools designed to ensure the security and non-vulnerability of all products and equipment. Supplier shall warrant that it will, for all products and equipment, implement fail-safe features that protect the product's critical functionality, even when the product's security has been compromised. Supplier shall provide _____ with a written copy of its Development Security Standards upon request and shall allow _____ personnel, or a third-party identified by _____ to view and assesses the standards. Supplier represents and warrants that, with respect to all of its products (as applicable), it meets and complies with all cyber-security guidelines and similar requirements and standards promulgated by any applicable regulatory body, where present.

Supplier can provide a third-party assessment of organization's product development as a validation of the process employed.

2. Security Program

Supplier shall represent and warrant that it has developed and continues to maintain a comprehensive written security program that contains administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of all of _____'s systems and data. Supplier represents and warrants that all audits and reports, produced as part of its written security program and all reports required to be produced or made available to _____ are able to be exported and delivered in electronic format. The supplier's written security program shall include, but may not be limited to:

a. Identifying and assessing reasonably foreseeable internal and external risks to the availability, security, confidentiality, and/or integrity of any and all supplier products, systems, servers, equipment, software, electronic, paper or other records. The written security policy shall include means of evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such supplied product(s) vulnerability and risks, including but not limited to:

   i. Ongoing employee (including temporary and contract employee) training;

   ii. Employee compliance with policies and procedures; and

   iii. Means for testing for, detecting and preventing security system failures on an ongoing basis.

b. Regular monitoring to ensure that the written security policy is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of _____'s systems and data, or any compromise in confidentiality, integrity, or availability of _____'s systems and data.

c. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of supplier products containing or which may access or be used to access _____'s networks, systems and data, or compromise the confidentiality, integrity, or availability of _____'s systems and data.

d. Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of _____.

e. Supplier can provide a third-party assessment of organization's security program as a validation of the process employed.

3. System Protection and Access Control

Supplier shall demonstrate that _____'s systems and _____ data are protected by appropriate network security controls that prevent

unauthorized access by providing _____ with network diagrams of supplier's environment used to provide products, equipment, maintenance and services to _____.

a. Supplier infrastructure - Supplier shall warrant that an incident response mechanism is in place for unauthorized access or disclosure of technology and assets on the supplier infrastructure. Supplier shall have an approved C level process for notification to _____ of unauthorized access or disclosure of technology and assets on the supplier infrastructure that may impact business operations of products and services delivered to _____.

b. Supplier shall provide _____ with a standard operating procedure for securing suppliers' technology assets with independent evaluation and assessment where applicable and a management audit of said standard operating procedure annually.

c. Communications between supplier and _____ shall be performed with a secure mechanism. Supplier shall provide operating procedures for secure mechanism to ensure no unauthorized access or disclosure of technology and assets.

d. All supplier products and services that have the capability to perform remote system maintenance, software upgrades, troubleshooting and diagnostics shall provide technical documentation on these capabilities which shall have the following at a minimum:

   i. Strong authentication mechanisms for access to products and services

   ii. Mechanism to perform any remote software downloads are:

      1. Validated as an uncompromised supplier deliverable

      2. Validated as an unaltered supplier deliverable

      3. Validated that only that action is performed

      4. Validated that it does not provide access to any other systems except for the purpose of updating the software to a supplier deliverable

   iii. Ability to prevent the introduction of any unwanted activity unauthorized by the supplier

e. Supplier agrees that no external access to their internal networks and systems, will be permitted unless strong authentication and encryption is used for such access. Supplier represents and warrants that all internet and network communications will be encrypted and authenticated. Any necessary external communications for purposes of service or maintenance functions to be performed by supplier will be encrypted and will utilize multi-factor authentication to access any and all devices, equipment and/or applications. Supplier shall maintain an access control list for all access to the internal network from an external network and supplier agrees that any of its servers exposed to the internet that contain _____ data or access _____ systems run on a hardened operation system.

4. Product Testing and Verification

Supplier shall perform a vulnerability assessment for any or all products that will be provided to _____ as part of a contractual agreement, including scanning, and penetration testing by a tester of _____'s choosing (or a tester selected by supplier and approved by _____) or, in _____'s discretion, _____ personnel may perform such vulnerability assessment, all at no cost to _____. Supplier represents and warrants that it performs security testing and validation for all of its products, and that all security testing performed by supplier covers all issues noted in the "SANS/CWE Top 25" and "OWASP Top 10" documentation, and shall include a vulnerability scan encompassing all ports and protocols. Supplier shall provide _____ with a test plan for all tests performed for review and approval by _____. The testing shall include, but not be limited to:

a. Communication Robustness Testing – This shall include, at a minimum, communication protocol fuzz testing to determine the ability to properly handle malformed and invalid messages for all identified communication protocols in the supplier product, as well as data resource exhaustion tests (aka "load

testing" and "DoS testing"). Communication robustness testing shall be performed using tools that are approved by _____, and that produce machine-readable data.

b. Software Composition Analysis – This shall include, at a minimum, an analysis of all compiled code found in the supplier product and shall identify all third-party open source components, and shall, at a minimum, identify all known vulnerabilities found in the Common Vulnerabilities and Exposures (CVE™) in publicly available databases. Software composition analysis shall be performed using tools that are approved by _____, and that produce machine-readable data.

c. Static Source Code Analysis – This shall include, at a minimum, an analysis of all available source code found in the supplier product and shall identify weaknesses enumerated by Common Weakness Enumeration (CWE™). Static source code analysis shall be performed using tools that are approved by _____ and that produce machine-readable data. All CWE Top 25 and OWASP Top 10 issues that have not been remediated must be clearly documented as an exception.

d. Dynamic Runtime Analysis – This shall include, at a minimum, an analysis of how the supplier provided software behaves during operation and whether such behavior introduces potential security vulnerabilities that could negatively impact confidentiality, integrity, and availability.

e. Known Malware Analysis – This shall include, at a minimum, a scan of supplier provided software to determine if any known malware exists in the supplier provided software and a risk assessment on mitigation controls or value of risk.

f. Bill of Materials – The supplier shall provide _____ a bill of materials that clearly identifies all known third-party software components contained in the supplier product. This shall be provided in a machine-readable format.

g. Validation of Security Measures – All security measures described in the product's design documentation are properly implemented and mitigate the risks associated with use of the component or device.

h. Third-Party Penetration Test – The supplier shall provide _____ with the results of a penetration test performed by a third-party penetration tester. _____ may, at their discretion, recommend a penetration tester of their choosing. The third-party penetration test shall, at a minimum, but not limited to, determine the following:

i. All ports and interfaces that the product has enabled and disabled for all configurations.

ii. All services that are external to the product for all configurations of the product. The test shall determine operational, service, test and non-functional services of the product.

iii. Measures implemented to prevent denial of service attacks on all ports, interfaces and services.

iv. All ports, interfaces, and services are documented and that there exists no undocumented port, interface or service.

v. All ports, interfaces and services that require authentication shall meet the requirements of the authentication section in the companion standard for the product ecosystem.

vi. Vulnerabilities in the product are probed and provide conceptual exploits to attack the vulnerability.

vii. Software and hardware weaknesses that are identified in the product that are in "SANS WE Top 25" and "OWASP Top 10" and/or otherwise negatively impact confidentiality, availability and integrity of the supplier product.

i. Risk Assessment – The supplier shall provide _____ with a threat model and subsequent risk assessment that includes, at a minimum, but is not limited to:

i. Risk criteria used to evaluate the significance of risk, including the level at which risk becomes acceptable.

ii. Risk identification, including (but not limited to) all known vulnerabilities identified through testing and all software weaknesses per "SANS WE Top 25" and "OWASP Top 10" publicly available lists.

iii. Risk analysis, including consideration of the causes and sources of the risks and their consequences.

iv. Risk evaluation, comparing the level of risk found during the analysis process with the established risk criteria to determine the acceptability of the risks.

v. Additional risk control measures shall be implemented to address all known vulnerabilities and software weaknesses that have been determined to present an unacceptable level of risk.

5. Deployment and Maintenance

Supplier shall provide _____ with detailed installation, deployment, and configuration instructions, and, at the request of _____ assistance in installation, deployment, and configuration that supplier warrants meets the expected security context resulting from meeting the requirements in this document. All supplied software products shall be authenticated through code signing. Supplier shall provide _____ with a stated lifecycle of supplied product and shall provide _____ with a maintenance plan that addresses both current and legacy products provided to _____. Supplier shall provide, at a minimum, but not be limited to, the following:

a. Ongoing Vulnerability Assessment – Supplier shall periodically apply all previously listed vulnerability assessment testing to the supplied products at a frequency of no less than once annually, and report any newly discovered vulnerabilities to _____ within 15 days of being discovered.

b. Patch Management and Deployment – Supplier shall design all products with the ability to apply patches when needed and shall provide _____ with the patch management plan. Supplier shall provide _____ with tested, verified, and validated patches in a timely manner, to not exceed 90 days for any vulnerabilities found in "SANS WE Top 25" and "OWASP Top 10", or any vulnerabilities deemed critical by _____. All patches and provided updates shall be authenticated through code signing.

c. Updates to Bill of Materials – Supplier shall provide _____ with an updated bill of materials per the previously stated requirement for any changes resulting from product updates, patches, etc.

d. End of Life – Supplier shall provide _____ with a disposition plan for all software that has reached the supplier stated end of life. This plan shall include, at a minimum, but may not be limited to:

i. Uninstallation instructions

ii. Removing of confidential information (e.g. data and keys)

iii. Transition plan to updated version of supplier product

iv. Supplier warrant that expected security context remains intact

About Synopsys

Synopsys, Inc. (Nasdaq:SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP, and is also growing its leadership in software quality and security solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest quality and security, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. The company is headquartered in Mountain View, California, and has approximately 113 offices located throughout North America, South America, Europe, Japan, Asia and India.

SYNOPSYS®

www.synopsys.com/software

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: sales@coverity.com