ERICSSON

Product Security Requirements for Suppliers

PSRS

Instruction

Preface

The Ericsson product security requirements for suppliers ("PSRS") represent the minimum product security and privacy requirements that the supplier, its affiliates, sub-suppliers and their personnel must adhere to when delivering products and services to Ericsson.

Supplier shall ensure that any additional requirements regarding security and privacy required as part of the relevant Agreement with Supplier and applicable laws and regulations are also complied with. More detailed requirements might be defined in relevant Specification connected to the agreement to which this PSRS will form part as an appendix.

This document is relevant for suppliers providing software components, and suppliers providing development services.

In addition, suppliers should consider external secure software development frameworks like NIST SSDF[1] to further evolve the secure software development processes and practices.

This document undergoes reviews on a regular basis and will be updated from time to time. The most recent version is available at Conditions and Guidelines - Suppliers & Partners - Ericsson[3].

Contents

1 Product Security and Privacy Requirements for Suppliers

Supplier shall provide secure products when delivering to Ericsson, by implementing applicable controls as set forth in this PSRS.

The product security and privacy requirements presented in this document are the minimum product security and privacy requirements that Supplier must adhere to when delivering hardware products when including software, software products or any combinations thereof (herein "Products") to Ericsson. These security and privacy requirements will be complemented with additional product security and privacy requirements for a specific product or service.

Communications to Ericsson regarding security incidents and new vulnerabilities shall be made to the Ericsson Product Security Incident Response Team ("PSIRT") at: psirt@ericsson.com.

2 Product Security requirements

2.1 Product security requirements for Products and components

The requirements in this chapter relate to the development and maintenance of the Products and components delivered to Ericsson as well as the characteristics, features and documentation of those.

2.1.1 Vulnerability disclosure

Supplier shall, without unnecessary delay, inform Ericsson PSIRT if they discover new security vulnerabilities or security incidents in or related to Supplier Products delivered or to be delivered to Ericsson, including security incidents impacting the design, development, manufacturing, delivery, installation or use of such Products.

The vulnerabilities should be communicated using CSAF [4] standard, version 2.0 or later, where Supplier acts as a 'trusted provider' as specified in the CSAF v2.0 standard. It is proposed that the communication is done through an API.

2.1.2 Vulnerability mitigation

A fix for a vulnerability must be made available to Ericsson according to the following timelines as per the severity of the vulnerability and as per type of code where the vulnerability has been discovered:

Type of code	Critical or known exploited vulnerability	High vulnerability	Medium vulnerability	Low vulnerability (CVSS <3.9)
Supplier proprietary code	10 days from discovery	20 days from discovery	40 days from discovery	120 days from discovery
Open source or other downstream third-party code	20 days from availability of third party provided fix	40 days from availability of third party provided fix	60 days from availability of third party provided fix	180 days from availability of third party provided fix

The days mentioned are business days.

The severity of the vulnerability shall be determined using the FIRST CVSS methodology, version 3.1 or higher. The severity score shall be determined by the supplier or a downstream third party with included reasoning provided via CSAF.

If the supplier or downstream third party does not provide a score, the NIST/NVD base score shall be used.

In the table above, the date of discovery of a vulnerability is the date when a finding is verified and decided by the owner of the Product to be a vulnerability.

2.1.3 Security Assurance

Supplier shall according to what Ericsson reasonably request:

a. adhere to a documented secure software development process. This process may be Supplier specific;

b. have a documented process for handling security patches and updates in a timely manner including performance metrics indicating the level of compliance;

c. continuously educate its staff on security related topics;

d. provide the technical security expert contact information to the contact person at Ericsson;

e. have a risk management process as part of the secure software development process including threat analysis, risk assessments and risk treatment plan on products and services;

f. follow secure coding best practices, in particular code configuration management, static code analysis and code peer review;

g. perform security testing including at least port and vulnerability scanning, web interface testing, fuzzing, configuration scanning, DoS testing and penetration testing;

h. deliver Product as pre-hardened, secure by default state.

2.1.4 Supply chain security

Supplier shall provide Ericsson with a bill of materials of Products and country of their origins, excluding open source, at the latest when they are delivered to Ericsson or its customer.

Supplier shall specify and document third party software components used and their respective version numbers, both open source and proprietary components, and provide Ericsson with a software bill of materials that conforms to the SPDX Specification V2.2.1/ISO 5962:2021 and to the SBOM specification for suppliers (see Conditions and Guidelines - Suppliers & Partners - Ericsson[3]) for all software that is to be delivered to or be made available for use by Ericsson or its customer.

Supplier shall avoid using vulnerable, tainted or unsupported components as part of the Products.

2.1.5 Documentation

In addition to the bill of materials mentioned in previous chapter, Supplier shall deliver to Ericsson product documentation containing a user manual/guide for security and possibly other Product documents that cover:

a. all features, commands and services in the Product;

b. hardening and troubleshooting functionality;

c. any other functionality/information that is necessary for the secure management of the Product.

Supplier shall deliver documentation about used vulnerability scanning tools as well as the results of the scans. This documentation shall be delivered to Ericsson for every Product Upgrade and/or on specific Ericsson request. The documentation shall include the false positive findings from the scanning tools, together with evidence of them being false positive.

As part of product release documentation, Supplier shall deliver details on the fixed and still present vulnerabilities in the release.

All vulnerability documentation must be made available using CSAF and describe, per vulnerability, at a minimum the following information:

1. The product name
2. The product version
3. The CVE
4. The CVSS 4.0 and 3.1 severity, base score, and vector. A CVSS 4.0 score is preferred over 3.1.
5. If the base score has been changed, the respective CVSS score(s), severity, vector(s), and reasoning must be provided
6. The vulnerability resolution status (CSAF specification 3.2.3.9)

Any vulnerabilities still present in the release must be accompanied by:

1. A VEX justifications as per CSAF Specification chapter 3.2.3.5
2. Reasoning why the vulnerability was not resolved in this release, and
3. A specific date and product version when a version of the product wherein the vulnerability is not present will be released to Ericsson.

Supplier shall deliver the documentation according to what Ericsson reasonably requires and for every Upgrade, or on request by Ericsson.

Supplier shall retain internal documentation about the Product that cover:

a. The security architecture of the Product;
b. Evidence of performing the security assurance activities;
c. Results from the security assurance activities performed.

2.1.6 Features

Detailed functional security requirements on the Products will be specified and agreed upon in the Specification. The detailed functional security requirements encompass basically the following six functional areas below. Examples of requirement topics for each functional area are also outlined below to illustrate the potential detailed requirements.

2.1.6.1 Network protection

This functional area covers requirements on e.g. confidentiality and integrity protection of operations and maintenance ("O&M") traffic and traffic separation.

2.1.6.2 Identity and access management

This functional area covers requirements on e.g. O&M user ID administration, password management and user authentication and authorization.

2.1.6.3 Logging

This functional area covers requirements on e.g. security event logging, support for both local and remote logging and full personal accountability.

2.1.6.4 Data protection

This functional area covers requirements on e.g. protection of passwords, confidentiality and integrity of personal data.

2.1.6.5 Application security

This functional area covers requirements on e.g. web application security and secure default values of parameters.

2.1.6.6 Platform security

This functional area covers requirements for e.g. software signing.

2.2 Product privacy requirements for Products and components

The requirements in this chapter relate to the Products privacy-specific documentation and features.

2.2.1 Privacy Assurance

Supplier shall according to what Ericsson reasonably request:

a. continuously educate its staff on privacy related topics;

b. provide the technical privacy expert contact information to the contact person at Ericsson;

c. perform a Privacy Impact Assessment on the product.

2.2.2 Documentation

Supplier shall deliver to Ericsson product documentation that

a. covers all privacy features and commands in the Product;
b. reports if the product is capable of processing Personal Data and in case it is capable, what is the data processed. The template for Personal Data Classification, found in Conditions and Guidelines - Suppliers & Partners - Ericsson[3], shall be used for this reporting.

Supplier shall deliver the documentation at agreed times, or on request by Ericsson.

Supplier shall retain internal documentation about the Product that cover:

a. Evidence of performing the privacy assurance activities;
b. Results from the performed privacy assurance activities.

2.2.3 Features

Detailed functional privacy requirements on the Products will be specified and agreed upon in the Specification. The detailed functional privacy requirements encompass, but may not be limited to, the following three functional areas. Examples of requirement topics for each functional area are also outlined below to illustrate the potential detailed requirements.

2.2.3.1 Personal data classification

This functional area covers requirements for e.g. classification of personal data.

2.2.3.2 Fair data processing

This functional area covers requirements for e.g. personal data tagging.

2.2.3.3 Personal data management

This functional area covers requirements for e.g. personal data retention.

2.3 Product Security requirements for Development Services

Supplier shall provide personnel (“Development Services Personnel”) with adequate and managed security and privacy competence to Ericsson, by ensuring a good level of training and assertion of the Development Services Personnel.

Work done for Ericsson shall be done in accordance with the Ericsson Security Reliability Model, and the project specific instructions. A good level of knowledge about the public version of the Security Reliability Model[2] is required for all the Development Services Personnel.

In general, the requirements for the service consist of three areas:

- Competence on the areas where Ericsson has the PSRS requirements;
- Competence on the (externally published) Security Reliability Model;
- Capability to implement Security Master Model as defined in 2.3.5.

2.3.1 Vulnerability handling

The Development Services Personnel shall have good knowledge of vulnerability handling, including how to manage information about vulnerabilities, how to triage a vulnerability and how to resolve a vulnerability in a timely manner.

2.3.2 Security Assurance

a. To have adequate knowledge of security and privacy aspects of the secure software development process, Supplier Development Services Personnel shall be continuously educated on security and privacy related topics;

b. Have undergone an up-to-date privacy training which encompasses privacy by design principles and best practices;

c. have good knowledge of risk management processes as part of the secure software development process including threat analysis, risk assessments, privacy impact assessments and risk treatment plan;

d. have good knowledge of secure coding practices, in particular code configuration management, static code analysis and code peer review;

e. have good knowledge of vulnerability analysis including penetration testing;

f. have good knowledge of hardening as a concept.

2.3.3 Other security requirements

Supplier Development Services Personnel shall:

a. Have good knowledge about architectural security and data protection principles;

b. Have good knowledge about supply chain integrity and the risks and mitigations on supply chain;

c. Have a good understanding and capability of documenting the work and the artifacts;

d. Have a good understanding of the common security and privacy controls in the areas of network protection, identity and access management, logging, data protection, application security, platform security, fair data processing and personal data classification and management.

2.3.4 Requirements related to the Security Reliability Model

Supplier Development Services Personnel should have good knowledge of the Security Reliability Model which is an Ericsson proprietary framework for ensuring security and privacy by design, as described in the public version of the Security Reliability Model[2] and be able to apply this knowledge in their area of expertise.

2.3.5 Requirements for Security Masters

Ericsson has implemented a concept called the Security Masters Model. According to the concept, all cross-functional teams shall have a security master appointed and trained. The exact implementation of the security master model depends on the Ericsson unit's specific descriptions and ways of working.

If the whole cross-functional team is sourced from Supplier, one of the Development Services Personnel needs to be appointed by the Supplier, who shall be trained as a Security Master, and they will be appointed to that job role. The training will be provided by Ericsson.

2.3.5.1 Security Master concept at Ericsson

The Security Master Model is a way to ensure that we have enough people across the whole organization, with the right competence, to execute on increasing security demands. Two new security roles are introduced in addition to the existing security roles: Security Master and Security Champion. Security champions are predominantly Ericsson personnel, but Security Masters can be Supplier personnel. Being a Security Master is a part time assignment added to the original job role. Security Masters are appointed and go through foundation training followed by a Qualification Exam. A Security Master focuses on driving security competence in their respective teams to continually improve the security posture of, as well as provide guidance on how to fulfil the security requirements for, the product, solution or service the team works on. The Security Masters also provide relevant security requirements, work instructions and guidelines as well as support compliance for the respective team, both internal within Ericsson and if needed within Supplier.

This means that the Security Master empowers knowledge sharing, competence and a learning culture aiming to enhance a security culture. It is essential that the master is eager to continuously develop competence as well as to have willingness and ability to work with people.

3 General Compliance

Without limiting other rights of Ericsson or obligations of Supplier according to the agreement entered:

a. Supplier internal audits and/or assessments concerning security and privacy shall be performed by Supplier regularly by trained personnel and findings shall be evaluated for possible corrective actions and reported without delay to Ericsson if they are likely to have any negative impact on Ericsson or its customers.

b. Upon 10 business days request from Ericsson, Supplier shall be able to demonstrate compliance with this document and any other security and privacy requirements or measures that have been agreed with Ericsson. Identified non-compliances shall be corrected promptly without additional cost to Ericsson.

4 References

[1] NIST SSDF, National Institute of Standards and Technology, Secure Software Development Framework
[2] External Security Reliability Model Description, Ericsson's external edition of the Security Reliability Model
[3] General Sourcing Conditions, Documents related to Ericsson's sourcing conditions
[4] CSAF, Common Security Advisory Framework

5 Definitions and Terminology

For the purposes of this document, the following words and expressions shall have the meaning assigned to them below unless the context would obviously require otherwise.

Specification	A set of detailed technical requirements for a specific product or service, such as but not limited to an assignment specification in a statement of work or similar.
Hardening	Hardening is a process of securing a system by reducing its attack surface. For example, hardening of a software component means removal of unused sub-components and services.
Privacy Impact Assessment	See https://gdpr-info.eu/issues/privacy-impact-assessment/
Product	Hardware products when including software, software products or any combinations thereof
Upgrade	A release of the Product leading to increased or modified functionality in respect of functionality included in the previous release
Personal Data	Personal data means data that can be used to directly or indirectly identify an individual person, e.g. demographics, MSISDN, IMEI, location, and IP address.

These terms and acronyms are used in this document.

FIRST	Forum of Incident Response and Security Teams, see https://www.first.org
CVSS	Common Vulnerability Scoring System, see https://www.first.org/cvss/
NIST	National Institute for Standards and Technology, see https://www.nist.gov/
NVD	National Vulnerability Database, see https://www.nist.gov/itl/nvd

