Product Security Incident Response Team (PSIRT)

ERICSSON

Executive summary

Ericsson Product Security Incident Response Team (PSIRT) is responsible for the Ericsson product vulnerability management process and the coordination of customer product security incidents affecting Ericsson products, solutions, and services. PSIRT is focused on the identification, assessment, and disposition of the risks associated with Ericsson products. PSIRT is involved when secure products are developed and used.

PSIRT actively collects vulnerability information from various sources and informs product development of its findings. Product development evaluates the relevance of a vulnerability and develops plans on how that vulnerability can be addressed. This leads to a better understanding of the security posture of each product version.

PSIRT assists the customer units to make sense of various security questions and prepare an informed response to resolve security issues. This is often done via the customer service request processes or less formal means, such as emails or news postings.

To be able to respond effectively to any product security incident, processes and experience must be put in place beforehand in a very similar way to other emergency or crisis management processes, and this is when PSIRT steps into the picture. Sometimes it may involve collecting the right team and delivering the solution in time. On other occasions, it may require arranging access to the site and securing the evidence.

Introduction

Modern telecom networks are a complex part of the critical infrastructure of our digital society. Security of the networks is essential for keeping critical services available and reliable. Unfortunately, seamlessly secure networks rarely exist, and security must be considered from the initial steps of product development until the end of the product's life cycle and even further in the life cycle management processes.

Almost any modern software consists of free open source and third-party components, so does software in networks. Therefore, processes of monitoring authenticity and security of the used third-party software and hardware are an increasingly important part of product security.

Ensuring the security of software in the highly dynamic and ever-changing security landscape is a continuous and evolving process. PSIRT has a central role in this at Ericsson.

Regular risk assessments, technical vulnerability assessments, and systematic vulnerability management are a crucial part of what Ericsson does to protect against security incidents. When someone suspects that an Ericsson product has a vulnerability that could be exploited, or an Ericsson product has fallen victim to a cyberattack, PSIRT takes the lead to investigate the situation and if needed, mitigate the incident.

PSIRT is a centralized team in the Ericsson CTO office. Centralized security expertise ensures that Ericsson can proactively address security issues, handle questions or incidents, and effectively respond. The efficient handling of an incident, especially if it involves sensitive information, benefits from a single point of contact (SPoC), which ensures coordination and effective flow of information.

PSIRT was established in 2004 and was accredited by Trusted Introducer (GEANT/TF-CSIRT) in 2005. PSIRT is a full member of FIRST, a global Forum of Incident Response and Security Teams, since 2006. PSIRT is active in co-operation with international Computer Emergency Response Team (CERT) communities, vendors, and many telecom operator Computer Security Incident Response Team (CSIRT) teams. PSIRT also works with the ETIS community of telecom professionals.

01 Main operations of PSIRT

PSIRT has two major operations: Vulnerability management and incident response. PSIRT also works closely with the internal Security Reliability Model (SRM) processes. PSIRT has a dedicated subteam to answer all customer service requests when it comes to security related questions. That guarantees the seamless flow of product security related information in the customer support organization.

Vulnerability Management

PSIRT's one main area of responsibility is providing a proactive vulnerability management service for product development units throughout the company. In a large and dynamically changing codebase, managing vulnerabilities is a delicate and complex task. Accurate and timely coordination between the vulnerability information sources, product development, customer support, customers—and on occasion, executives and public relations—is handled by PSIRT. Awareness building across the company on current and upcoming security phenomena related to product development is on the task list of PSIRT as well (for example through the Security Masters program).

Upon receiving a security alert, the product development unit will analyze the vulnerabilities listed in the alert and initiate a procedure for remediation. According to the global process, the product development unit responds with a mitigation plan and timeline.

The process described above is supported by an in-house vulnerability management system, which allows PSIRT to accurately map new vulnerabilities to the Ericsson portfolio.

PSIRT is using open industry standards in the vulnerability management process. These are CVE (Common Vulnerabilities and Exposures) for identification of vulnerabilities, CPE (Common Platform Enumeration) for structured naming of open source and commercial software,

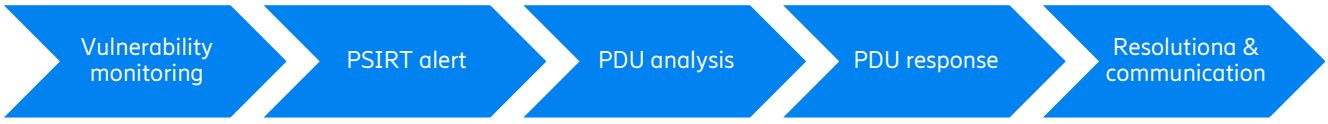

Figure 1: PSIRT vulnerability management process (PDU = Product Development Unit)

Ericsson products use various third-party components, both open source and commercial. When a new vulnerability could potentially affect an Ericsson product, PSIRT makes an initial vulnerability analysis and creates a security alert that is then sent to relevant security contacts of the product development unit. Every year, PSIRT processes thousands of vulnerabilities, and a subset of these vulnerabilities result in security alerts being created for the product development units.

and CVSS3 (Common Vulnerability Scoring System v3) for presenting the overall vulnerability impact and severity. CVE system is maintained by MITRE organization, while CPE scheme is maintained by NIST (U.S. National Institute of Standards and Technology). FIRST organization (Forum of Incident Response and Security Teams) is responsible for CVSS3 specification.

Incident Response

PSIRT acts as a single point of contact – for internal and external queries – when it comes to product security matters. In general, PSIRT will coordinate a response to any question related to the security of the Ericsson product portfolio.

The benefits of having a centralized incident response unit are clear. PSIRT's ability to reach the product owners, the security contacts and senior management prevents the information from getting lost between the cracks. Constant communication with other internal security organizations is also guaranteed through well-established processes and procedures.

If an event is categorized by any stakeholder as a security or privacy incident and involves Ericsson products, PSIRT will ensure that the case is investigated appropriately.

PSIRT defines an event as a product security incident if the following conditions are met:

1. The event is categorized by any stakeholder as a security incident
2. The event involves Ericsson products, solutions, or 3PPs provided by Ericsson

Figure 2: Definition of a product security incident

02 PSIRT incident handling process

PSIRT's incident handling process follows industry best practices based on NIST SP800-61 (Computer Security Incident Handling Guide) and ISO/IEC 27035 (Security Techniques—Information Security Incident Management) and is aligned with SANS Incident Handler's Guidebook.

All security incidents are managed according to the incident handling process depicted in Figure 3. In the triage phase, PSIRT ensures that the reported event is classified as a product security incident, urgency and criticality of the issue are identified and it is prioritized accordingly. At the start of the investigation phase, the investigation team is set up depending on the nature of the case, all major functions and departments (Crisis Management, Group Communications, Group Security, IT Security) are involved if necessary. PSIRT also ensures that the coordination is effective and business owners and decision makers are aware of the situation. Special attention is paid to collecting and preserving as much evidence as possible. The investigation team then proceeds to determine the scope of security and privacy impact based on the collected body of evidence. Containment efforts are started immediately after the impact analysis to avoid further damage and to deter malicious actors. A root cause analysis is done in parallel to devise both a short-term and long-term recovery plan to eradicate the threat and secure the systems under investigation. Once the systems are successfully recovered and adequately secured, the learnings from the investigation are shared with all concerned parties to avoid similar incidents in the future and to improve Ericsson's product security. PSIRT also uses the findings and lessons learned from these investigations to improve its own processes. The order of activities undertaken in each step depicted in Figure 3 can vary in real investigations due to the diverse nature of incidents handled by PSIRT.

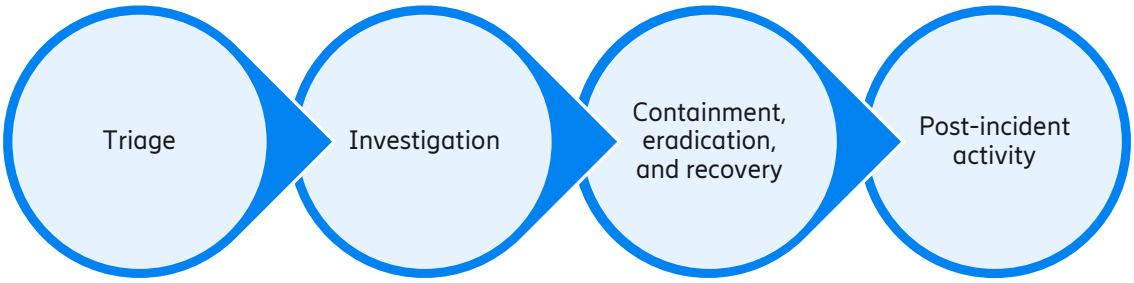

Figure 3: PSIRT incident handling process

External vulnerability disclosures

Ericsson has a responsible disclosure policy, through which PSIRT acts as a single point of contact for security researchers external to Ericsson if they discover a vulnerability in an Ericsson product or service. PSIRT's vulnerability disclosure policy and ways of working are based on ISO/IEC 29147 standard.

Vulnerability disclosures handled by PSIRT vary in complexity. An active dialog between Ericsson and the researcher in such cases is essential to resolve the reported vulnerabilities. Therefore, PSIRT internally coordinates the technical resolution of reported vulnerability while ensuring that

communication with the researchers is in place during the whole process, from the point of informing Ericsson to the point where a fix is delivered.

Product support for customers

PSIRT also has an important role in the Ericsson global support and engineering task force that provides customer support on product related questions. Customer questions that are related to security or privacy can be assigned from any place in the world into the PSIRT security support queue. These support requests are further analyzed and resolved in cooperation with the best security experts from product development and PSIRT. Customer requests may be related to hardening or configuration aspects, as well as the security status of software components used in Ericsson products.

03 Feedback loop for continuous improvement

In a large company like Ericsson, having established processes is key. Quality supports security, but it cannot exist without an efficient feedback process from customers and product development teams. From a security perspective, PSIRT ensures the effectiveness of this feedback loop.

When it comes to vulnerability management, PSIRT is automatically part of the process flow, from alerting to validating the alert answers sent by the product development units. The vulnerabilities have typically been estimated and scored by external security researchers to reflect their impact and relevance. Translating this estimate to the telecom context is challenging and requires an understanding of the context where the products will be deployed. PSIRT supports this learning process by giving feedback to product development based on extensive experience in the field.

As part of PSIRT's incident handling and vulnerability management capabilities, PSIRT is available to answer customer service requests in cases of security concerns. This ensures that Ericsson actively learns from different threats and concerns presented by customers.

Moreover, PSIRT actively contributes to other security assurance processes such as risk assessments and technical vulnerability assessments. PSIRT supports product development units and assists with the implementation of Ericsson's internal SRM by providing guidance on how to perform a solid vulnerability test and produce robust hardening guidelines.

PSIRT is composed of experienced, well-trained security specialists and the work is all about ensuring that network products developed by Ericsson are secure today and will remain secure in the future. Challenges of complexity and continuous change are the bread and butter for PSIRT and are dealt with daily.

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

Ericsson.com

1/287 01-FGB 1010955