Position paper - Vulnerability management

October 2022

Executive summary

This position paper aims to unpack the complexity and expand on the nuances of vulnerabilities, their role in a cyber-attack, and what from an Ericsson perspective constitutes the most effective mitigations. The end goal always being that the number of and impacts from cyber security incidents is minimized. This will ensure that resources are put to best use so that society can maximize the benefits new digital innovations bring about.

Commonly understood, a vulnerability is a weakness in software that can be exploited resulting in the compromise of security and privacy. But vulnerability can also be caused by the misconfiguration of a system, a lack of hardening of software products, or a flawed architecture. In other words, anything that introduces a weakness that can be exploited by a third party is considered a vulnerability. Consequently, it is incorrect to conflate the meaning of a vulnerability as just a software weakness that can be exploited.

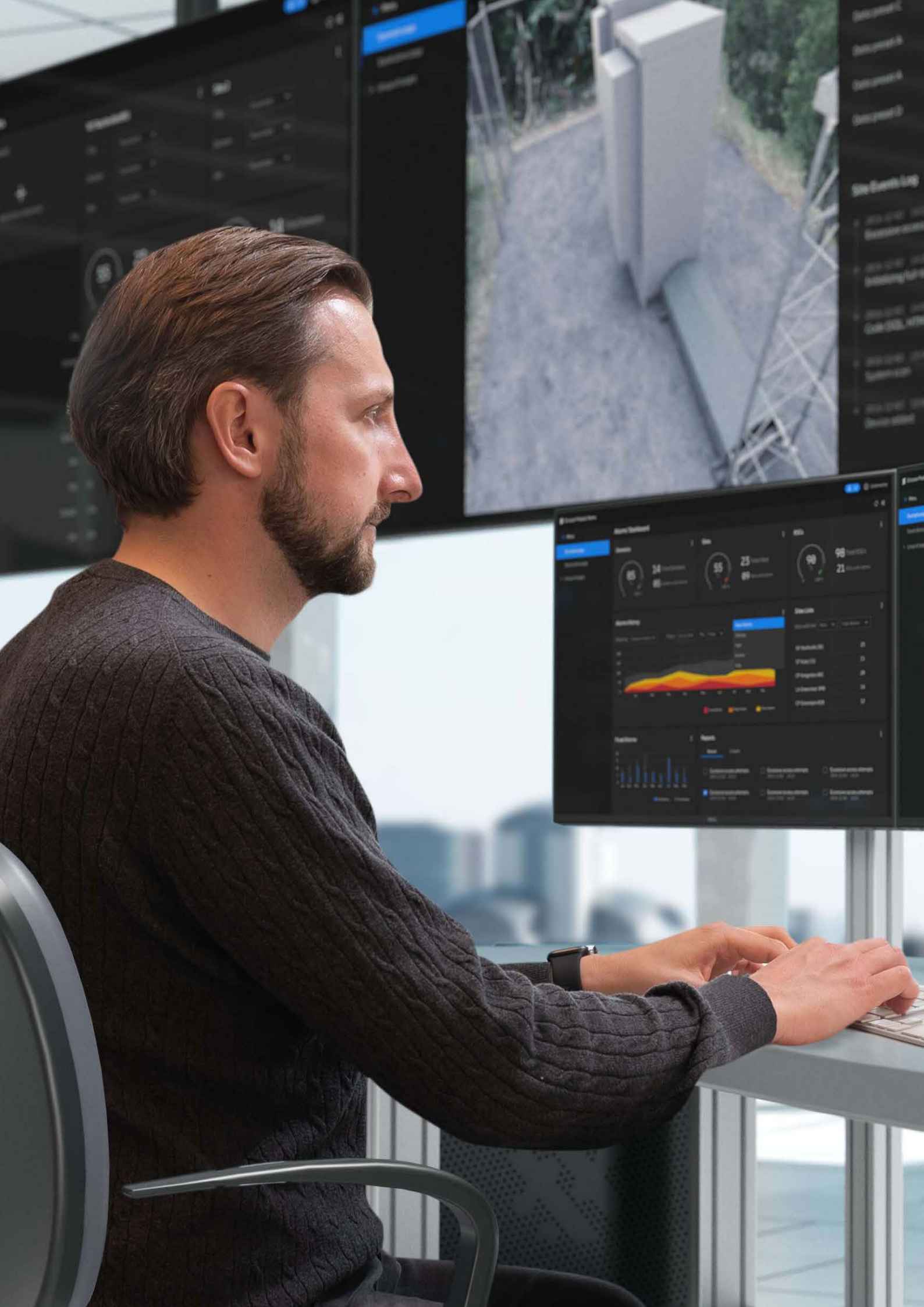
The different stages and steps of a cyber-attack are often described as a cyber kill chain and software vulnerabilities offer only one option for the attacker in the kill chain. Often the presence of a software weakness is not a sufficient condition for successful exploitation and the associated negative consequences to materialize.

To help identify the severity of a vulnerability, the cybersecurity community has developed a globally recognized standard that helps contextualize and categorize software vulnerabilities. To help identify which vulnerabilities need to be prioritized the standard has measures to assess the context of a vulnerability by classifying the environmental and temporal security relevant criteria. This contextual environment requires the handling of vulnerabilities in a risk-based manner.

Ericsson has developed the "trust stack" concept, which models the security posture of a deployed network. Due to the multifaceted, multivendor, and highly interdependent context of how telecom networks are realized to deliver end-user services, executing a successful attack is not trivial in networks with appropriate security hygiene. A successful attack on a deployed telecom network would require multiple security controls and processes to fail to create the opportunity to exploit a software weakness.

Without an all-encompassing approach to cyber security, from development to operations, security incidents cannot be minimized. The standards, frameworks, and technology already exist, but these need to be put to appropriate use. When developing a public policy response, careful consideration is essential to recognize vulnerabilities in the relevant security context, which significantly differs across consumer, enterprise, and telecom networks.

Therefore, a holistic, risk-based, and well-targeted regulation is best suited to ensure a secure and resilient critical infrastructure. Fragmented or disproportionate emphasis on silver bullet solutions risks creating a false sense of security and a risk of diversion of valuable security resources to fix vulnerabilities that are neither severe nor exploitable or necessary to execute a successful cyber-attack. The main consideration will be to minimize cyber incidents as opposed to minimizing the mere presence of any kind of vulnerability.



Introduction

The vast benefits from the continued digitalization of economies and society, driven by technologies such as 5G, Cloud, and IoT have also resulted in increased value at stake. This is a consequence of a combined effect of the increased amount of sensitive data that is being generated, transmitted, and stored. Along with an acceleration of cybercriminals and nation states willing to attack, extort, blackmail, or sabotage the internet, devices, IT systems, and critical infrastructures, the risks are as high as ever. This has led to a growing concern about the security and resilience of our digitized world. However, these threats and risks are not new, and mitigations are well known. It is important to consider gaps and missing incentives in implementing mitigations for business leaders and policymakers when developing public policy responses.

The field of cyber security is broad, technically complex, and without single silver bullet solutions, making effective and proportionate policy development and implementation difficult. One enduring discussion among policymakers and industry stakeholders is how to improve the detection, mitigation, and resolution of vulnerabilities. Some policymakers promote an enabling and fostering approach for the business environment to decrease vulnerabilities through voluntary action, which, in turn, contributes to a more secure digital ecosystem. At the same time, others consider regulatory interventions to regulate the vulnerability management process to achieve the same purpose.

However, vulnerability management is not a one-size-fits-all, nor a binary topic but rather one of nuance and appreciation of complexity. This position paper aims to unpack this complexity and expand on the nuances of vulnerabilities, their role in a cyber-attack, and what from an Ericsson perspective constitutes the most effective mitigations. The end goal always being that the number of and impacts from cyber security incidents is minimized, which will ensure that resources are put to best use so that society can maximize the benefits new digital innovations bring about.

What is vulnerability?

Commonly understood, a vulnerability is a weakness in software that can be exploited resulting in the compromise of security and privacy objectives [1]. A weakness can also be referred to as a bug or an error made in software code, which could be abused (that is, exploited) leading to a software vulnerability. Even more, what is not so commonly understood is that a vulnerability can also be caused by the misconfiguration of a system, a lack of hardening of software products, or a flawed architecture. In other words, anything that introduces a weakness in a computer system that can be exploited by a third party is considered a vulnerability. Therefore, it is incorrect to conflate the meaning of a vulnerability as just a software weakness that can be exploited.

Vulnerabilities also come in different classes, the most critical when exploited would result in an attacker obtaining privileged access to a system without any prior credentials. Most vulnerabilities, however, are typically less severe and require additional investment from the attacker to gain insight, privileges, and access to be able to successfully exploit. To help identify the severity of a vulnerability, the cybersecurity community has developed a globally recognized standard that helps contextualize and categorize software vulnerabilities. This de-facto standard, called CVSS – Common Vulnerability Scoring System [2], provides a set of criteria that are used to calculate the severity scoring of a vulnerability between 0.0 (none) to 10.0 (critical).

As an example, the Log4Shell [3] vulnerability had a CVSS score of 10.0, when it was discovered in December 2021 and received significant global media attention. That year alone, 1,053 out of a total of 24,399[4] , or about 4%, publicly disclosed vulnerabilities received the same critical classification. However, almost none of these additional critical vulnerabilities gained as much media attention. Log4Shell by itself is not a remote code execution vulnerability, and there are additional dependencies, such as how the affected software code is written and configured. As such, these contextual factors significantly impact if and how the Log4Shell vulnerability can be exploited. For this reason, despite the global attention and active exploitation [5], no major incidents were observed anywhere[6]. It brings us to the question of why vulnerabilities are not treated equally and why policymakers need to adopt a risk-based approach to vulnerability management to ensure that the industry continues to focus resources on vulnerabilities that are likely to result in cyber incidents.

Not all vulnerabilities are equal!

Vulnerabilities that allow an attacker to execute an attacker's own code in a system remotely without credentials (for example, through the internet) are the most severe class of vulnerability. Assets (a fancy word for targets prone to a cyber-attack) that are unprotected from remote code execution vulnerabilities and have significant exposure (such as when directly connected to the internet), needs the utmost priority to have mitigations applied.

Internal systems with the same vulnerability should also be prioritized for mitigation but with a lower priority. The nuance between these two situations is that for threat actors to exploit these internal systems, they must first have to defeat multiple security controls also known as 'defense-in-depth'. A defense-in-depth approach ensures that if one control fails, others will prevent an attacker from reaching their desired objective. This is the best practice when securing a computer system. Ultimately, it means that the same technical vulnerability in an internal system with defense-in-depth significantly increases the difficulty to exploit and therefore, is less likely to result in a cyber incident. So, policymakers need to balance their attention between the class of vulnerabilities and the presence of defense-in-depth measures.

Another notable vulnerability type is "privilege escalation," where attackers can exploit a weakness to elevate their access privileges from a lower privileged user (for example, a read-only user) to a high privileged user, often with the intention to gain administrator rights. For this type of vulnerability to be abused, an attacker first needs to gain initial access to the targeted system, either through phishing, reusing, or guessing passwords or by abusing a software vulnerability. Given these conditions, privilege escalation vulnerabilities are generally scored lower than remote code execution vulnerabilities.

To help identify how vulnerabilities should be prioritized the CVSS standard has measures to add the necessary context. This is because the **base** CVSS score (as often discussed in the media) only considers the vulnerability in isolation. In reality, computer systems or telecom networks are implemented in a security context that uses layers of protective measures such as firewalls, anti-malware, configuration hardening, and two-factor authentication measures. This security context is captured in the CVSS standard by classifying the environmental and temporal security relevant criteria:

- The **environmental situation is scored** by contextualizing the vulnerability in a specific environment regarding the sensitivity of the information, availability, and criticality of the system, and the integrity of the data. It also considers the exposure (for example, internet facing), if the system is monitored and administered by security professionals as in the case of telecom networks, or not as in the case of most consumer products, and how access to the system is controlled. In other words – by considering the value of the defense-in-depth measures that have been implemented it is possible to determine the actual risk in a specific situation.
- The **temporal score** quantifies the temporal or timely aspects of a vulnerability. After the discovery of a vulnerability, documentation, and tools for exploitation become available, but also mitigations and patches mature. Both factors respectively increase or decrease the risk of a vulnerability. If a vulnerability is found but no tools or code are known that can abuse the vulnerability the risk of the vulnerability being exploited is reduced. It is due to the logic that the chance of an attack being successful is reduced as it requires special research and knowledge. The same logic goes for when temporary mitigation is available. While the vulnerability might still be present in the code the chances of an attacker being able to abuse the vulnerability are reduced.

When the CVSS score is complemented with the environmental and temporal scores, it helps to assess the **risk score** [7] for a vulnerability in a particular system at a particular point in time. Taking the previous example, Log4Shell – this vulnerability was at the beginning given the highest CVSS scoring of 10.0 – with the assumption that affected systems were internet facing. However, when the very same vulnerability was calculated for a telecommunication system, where environmental factors ensured that there was no way for an attacker to breach the layered security controls (a required dependency for exploiting this vulnerability), the scoring and therefore, the risk was much lower.

Additionally, in the past five years, no major incidents have been reported to Ericsson's Product Security Incident Response Team (Ericsson PSIRT) that were caused only by a software vulnerability. Most of the reported incidents were caused by failed (basic) operational security control and hygiene in telecom networks. Furthermore, the annual report from ENISA [8] on Incidents in Telecom security, only identified a single incident caused by a software vulnerability. This finding is also corroborated by the annual report from Verizon [9] based on their incident response work where only 7% of incidents can be related to software vulnerabilities.

These findings might seem counter-intuitive when reading the news about vulnerabilities in the media because: not all vulnerabilities are created equal and both environmental and temporal factors matter. Experts who protect systems and telecom networks, as well as policymakers, need to adopt a targeted and measured approach to ensure that any intervention yields net benefits. When developing policy, careful consideration is essential to recognize a vulnerability in the relevant security context, which significantly differs across consumer, enterprise, and telecom networks. The foremost consideration needs to be that a one-size approach does not fit if the ultimate policy objective is to minimize cyber incidents as opposed to minimizing the mere presence of any kind of vulnerability.

What does it take for an attack to be successful?

The different stages and steps of cyber-attacks are often described as a cyber kill chain and clearly expose the difference between different kinds of vulnerabilities. Kill chains are methods that can be used to assess how a threat actor gains initial access, moves laterally into adjacent systems, and in the final step executes the attack, such as exfiltrating data, sabotaging, or maintaining persistence for subsequent objectives.

An initiative called "MITRE ATT&CK [10] " provides a standardized framework that models attacker tactics, tools, and procedures (in short TTP). In this framework, exploitation of a software vulnerability is one of many documented methods attackers may employ. Exploiting software vulnerabilities has limited value when considering the other options (vulnerabilities) made available to an attacker, such as:

- Phishing (for example, tricking a user to enter their password into a fake website),
- Password spraying (reusing credentials obtained elsewhere and attempting to use them on multiple systems to determine if they are valid),
- Scanning for network misconfigurations to gain access to adjacent networks or systems,
- Reusing legitimate software for malicious purposes ("Living off the land"),
- Abusing intended software functionality for malicious purposes, or
- Backdooring software (supply chain attack).

In summary, software vulnerabilities offer only one option for the attacker in the kill chain. A vulnerability is not alone on a piece of software but is part of an entire software package, running on an operating system, on a network, within a data center, and providing a specific service. It is this contextual environment that requires handling vulnerabilities in a risk-based manner and where CVSS helps to quantify the risk.

To further clarify the telecom-specific contextual environment, Ericsson has developed the "trust stack" concept, which models the environment from both a technical and ownership view. These four processes, as shown in Figure 1, are separate but interdependent, as the security of a deployed network is enabled by the previous process but made effective by the next process.

Any measure not implemented or implemented with a (software) weakness constitutes a vulnerability in the overall environment. These weaknesses when deployed in the network can later be abused by an attacker and together are the cause of security and continuity incidents.

Security of deployed networks
Ericsson Trust Stack model

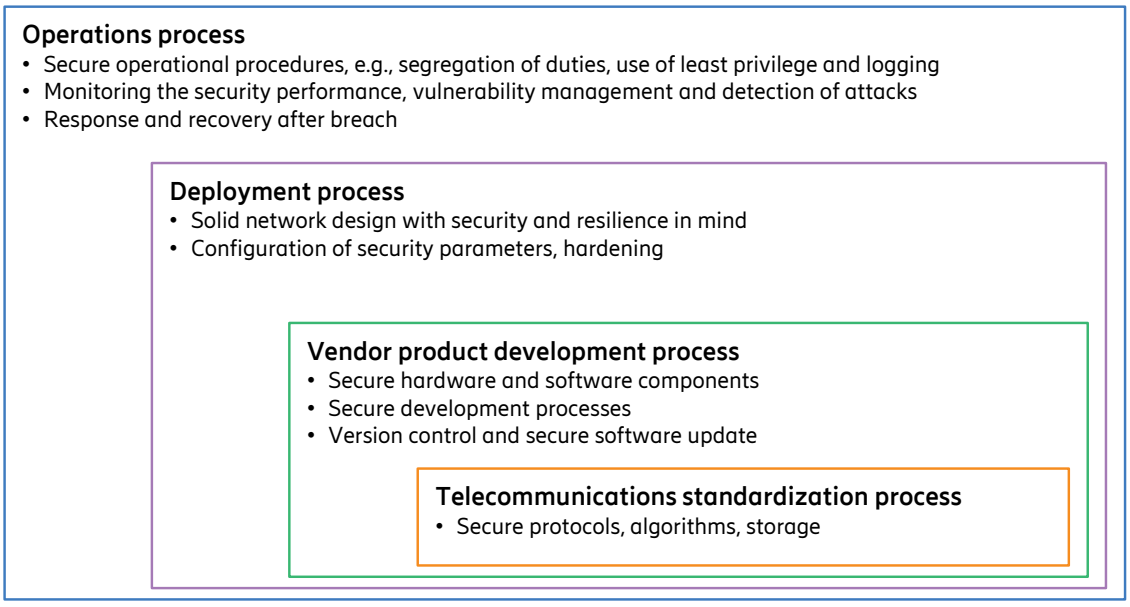


Figure 1- Ericsson Trust Stack model

What does it take to exploit a software vulnerability in a telecom network?

Often the presence of a software weakness is not a sufficient condition for successful exploitation and the associated negative consequences to materialize. A successful attack on a deployed telecom network would require multiple security controls and processes to fail to create the opportunity to exploit a software weakness deep inside the network.

Due to the multifaceted, multivendor, and highly interdependent nature of how telecom networks are realized to deliver end-user services, executing a successful attack is not trivial in networks with appropriate security hygiene. The security posture of a deployed network (see also figure 1) depends on:

- Standards used by vendors to develop products,
- The unique per vendor product development processes, including sourcing or development of hardware components, third-party software, open-source software, and in-house software development,
- The configuration of discrete final network components to a complete network (or more likely installment into a legacy network),
- Daily operations of deployed networks including threat detection and mitigation.

High level mobile network overview

Logical elements and logical planes

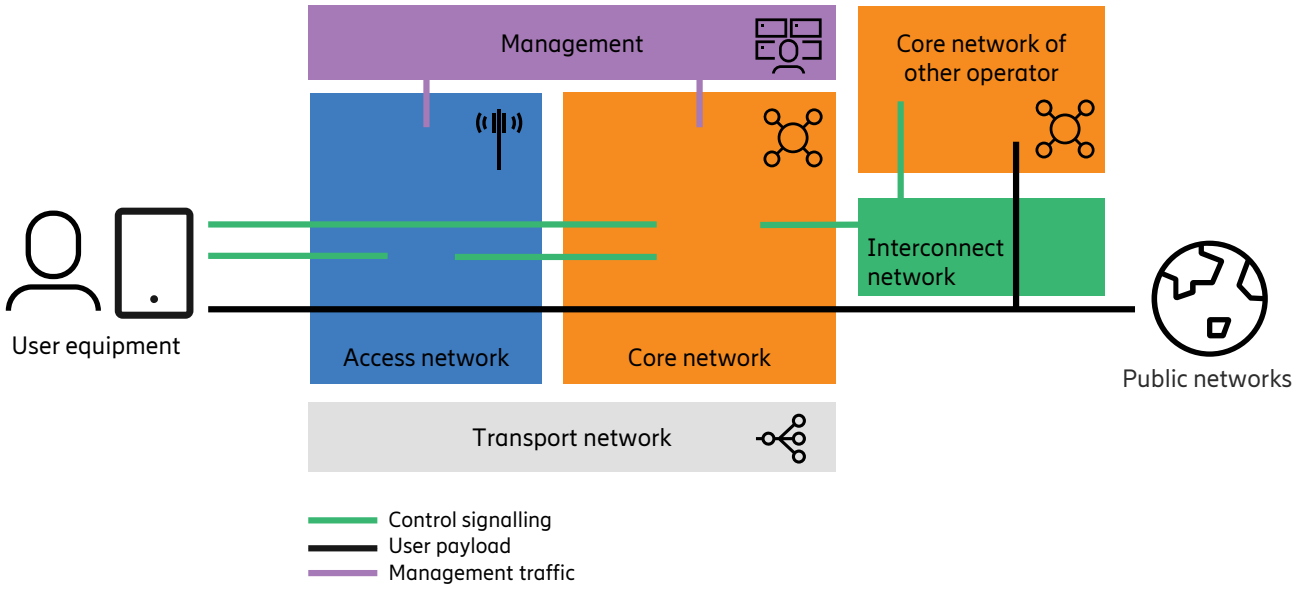


Figure 2 High level mobile network overview

As shown in Figure 2 Telecom networks are segmented into different domains such as Radio, Core, and Management with the equipment that facilitates the different generations (2G, 3G, 4G, 5G) deeply interconnected. However, from a user perspective, these systems are fully transparent (not accessible to the user of a mobile system), and access to networks is minimal and protected by strict defense-in-depth measures configured by the communications service provider (CSP).

This design makes the exploitation of a vulnerability – especially the ability to obtain persistent privileged access – strongly dependent on the protective measures in place in the systems and the network. Furthermore, if these protective measures are compromised, an attacker has many options far beyond software vulnerability exploitation that also require less investment to achieve a broader set of objectives. This is not to say that the minimizing of critical software vulnerabilities is undesirable. It is necessary, of course, but not sufficient if the ultimate objective is to minimize cyber incidents. Rather, system vulnerabilities and effectiveness of protective measures, for example, defense-in-depth matters a lot and at minimum needs to be considered by policymakers when developing vulnerability management policy frameworks.

What is in the control of a telecom network manufacturer?

The manufacturers of telecom equipment must of course have a process to handle vulnerabilities throughout the entire life cycle (figure 3). This is to appropriately deal with the discovery of new vulnerabilities as much as target resources at the most relevant vulnerabilities to mitigate the possibility of cyber incidents to occur.

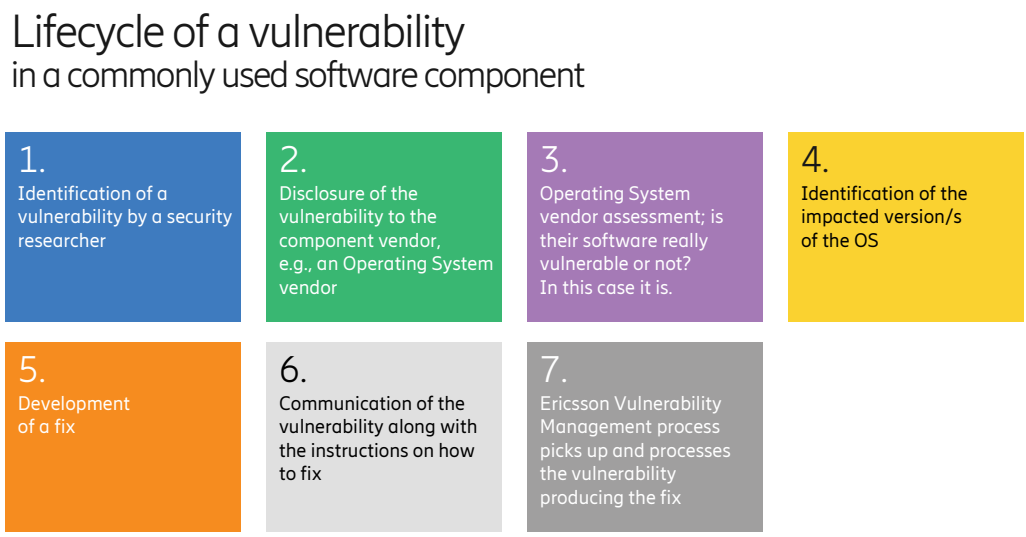


Figure 3 - Lifecycle of a vulnerability

In addition to minimizing the creation of new vulnerabilities, manufacturers need to implement multiple measures that together help ensure the development of secure products. Ericsson has established an internal control framework known as the Security Reliability Model (SRM) [11] depicted in figure 4.

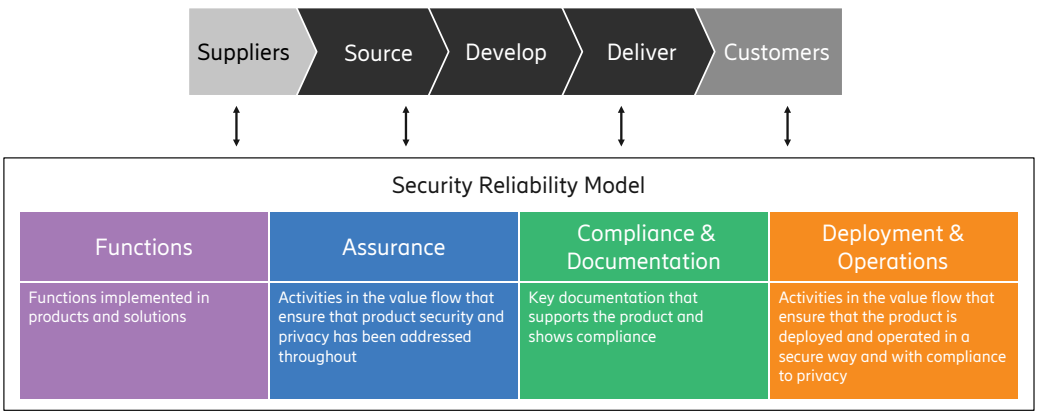


Figure 4 Ericsson's Security Reliability Model

The SRM enables managed, risk-based software development processes to ensure security and privacy implementation of requirements tailored to the target environment (context) and demands. Contained in this framework are the processes of vulnerability management as shown in distinct phases in Figure 3.

The time needed for each phase depends on the severity of the finding. While Ericsson provides context-specific information to its customers on how to configure, deploy, and operate products with targeted security, the control over such security-relevant decision-making is outside the control of a manufacturer.

Recommendations to policymakers

The following key attributes merit managing vulnerabilities differently in the context of telecom networks compared to consumer devices or enterprise (corporate) IT networks:

- Criticality of the system
- Active security management and monitoring of the system
- Bilateral communication channels for vulnerability disclosure

Rather than aiming to remove all vulnerabilities (which is impossible to achieve), the most effective measure is to take a holistic approach and ensure that security best practices are implemented at all levels of the trust stack (figure 1). Doing so guarantees that systems are protected against all types of attacks, apart from targeting software weaknesses for improving overall security and minimizing the risk of a security or continuity incident. Policymakers can contribute by defining the overarching security outcome objectives and ensuring that international/ global standards are applied to foster conducive market conditions. Government authorities can help by sharing information about threats and incidents in an appropriate way.

Regarding vulnerability management in the context of telecommunications networks to achieve the objective to minimize the number and impact of cyber security incidents, Ericsson suggests the following to be considered:

1. Define and implement a multiparty 'Common Vulnerability Disclosure' (CVD) process including all relevant parties to standardize the exchange and resolution of vulnerabilities.

2. Ensure that system vulnerabilities and software vulnerabilities are addressed in an all-encompassing way, thus avoiding fragmented approaches. Obligations should be symmetrical for all security-relevant stakeholders.

3. This is achieved by providing all responsible parties in the trust stack with a strong enough incentive to implement the required processes and tooling to minimize weaknesses during standardization[12] , development, deployment, and operation.

    a. It will also ensure that the number of and impact from cyber security incidents is minimized far beyond the presence of critical exploitable vulnerabilities.

4. Implement effective and proportionate means for validating that all parties have fulfilled their responsibility and implemented the required processes.

A CVD process resolves many of the issues pertaining to vulnerability disclosure namely:

- Technical details regarding critical software vulnerabilities are often considered initially sensitive as premature disclosure might result in attacks by threat actors before mitigation is available,
- The defenders often require technical details of the vulnerability to be disclosed to them to adequately protect their systems,
- Defenders require time to test and deploy patches or mitigations, and
- The severity or impact of a vulnerability is not always directly clear. Disclosing uncertain, ambiguous, unreliable information can add confusion, increase the time to implement a patch or mitigation, and impose unnecessary costs on defenders.

To counteract the issues above, a multiparty CVD process is necessary. The process ensures that all necessary parties are informed of the new vulnerabilities and mitigations, ensuring communication timelines and response resolution times are synchronized between all relevant stakeholders. Two organizations, FIRST [13] and OECD [14] both provide valuable frameworks to facilitate such a process.

What a CVD process does is facilitate the reduction of the overall risk of a possible incident. As explained above, a company with good security hygiene incorporates multiple security controls to reduce the probability of an incident occurring, or the impact if an incident does occur. If the goal is to have critical infrastructure that is secure and resilient against cyber-attacks, then all parties in the trust stack must implement the relevant security best practices. Any public security policy needs to ensure that all parties are incentivized and covered by obligations within their sphere of influence to be held accountable for outcomes. The number of vulnerabilities can be reduced, and incidents prevented by setting and validating clear guidelines for which best practices must be implemented to counteract threat(s).

Without an all-encompassing approach to cyber security, from development to operations, security incidents cannot be minimized. The standards, frameworks, and technology already exist but they need to be put to appropriate use. Therefore, a holistic, risk-based, and well-targeted regulation is best suited to ensure a secure and resilient critical infrastructure. Fragmented or disproportionate emphasis on silver bullet solutions risks creating a false sense of security and a risk of diversion of valuable security resources to fix vulnerabilities that are not severe, exploitable, or necessary to execute a successful cyber-attack.

Reference

1. https://cwe.mitre.org/about/faq.html#A.1
2. https://www.first.org/cvss/
3. https://en.wikipedia.org/wiki/Log4Shell
4. https://www.cvedetails.com/cvss-score-charts.php
5. https://blog.cloudflare.com/exploitation-of-cve-2021-44228-before-public-disclosure-and-evolution-of-waf-evasion-patterns/
6. https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf
7. The calculation for determining 'risk' is simplified by chance multiplied by impact. The chance of something happening versus how bad the results determine the risk – ergo how fast you want to fix the underlying issue. The CVSS method helps to quantify these parameters.
8. Telecom Security Incidents 2021 — ENISA (europa.eu)
9. 2022-data-breach-investigations-report-dbir.pdf (verizon.com) - Figure 35, Figure 40, Page 31
10. https://attack.mitre.org
11. The Ericsson Security Reliability Model
12. ETSI - Coordinated Vulnerability Disclosure (CVD)
13. https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1
14. https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf

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