Enhancing Vulnerability Management in Cybersecurity Certification: Leveraging Attack Potential and CVSS score

Mirko Malacario[1,*,†], Samuela Persia[1,†] and Ivan Di Pietro[1,†]

[1]Agenzia per la Cybersicurezza Nazionale (ACN), Corso d'Italia 41, 00198 Rome, Italy

Abstract

Due to the rapidly evolving scenario of the emerging IT technologies, the need for effective tools to strengthen the cybersecurity posture of the digital ecosystem has become critical. Cybersecurity certification can act as a cornerstone for providing assurance in product security, thereby fostering trust and promoting systemic cyber resilience within the market. Achieving a good balance between the need to obtain the assurance, through a cybersecurity certification, and the need to maintain an IT product updated, is increasingly critical in today's dynamic technological landscape.

For this reason, in the context of European cybersecurity certification, vulnerability handling has become a key factor in cybersecurity certificate maintenance activities.

This paper explores a possible approach to vulnerability classification and handling within the first European cybersecurity certification scheme, EUCC (EU Cybersecurity Certification Scheme based on Common Criteria), by leveraging existing international frameworks for vulnerability classification, such as CVSS (Common Vulnerability Scoring System) score, to automate the process of Common Criteria attack potential calculation starting from a published CVE (Common Vulnerability and Exposures).

This approach enables risk owners to prioritize the management of those discovered vulnerabilities, by establishing, through the correlation of CVSS score with attack potential, a risk acceptance level using residual vulnerability concept, ensuring timely remediation of newly discovered vulnerabilities and the maintenance of the cybersecurity certification validity.

Keywords

Cybersecurity, ICT Certification, Common Criteria, Attack Potential, Common Vulnerability Scoring System, Common Vulnerability and Exposures, Vulnerability Handling, Cybersecurity Act,

1. Introduction

In the last decade, the rapid evolution of emerging technologies, such as 5G mobile networks, edge computing, cloud infrastructures, and Artificial Intelligence, has increased the proliferation of highly interconnected devices. This technological convergence enabled the realization of large-scale applications through different domains such as healthcare, industrial systems, and energy management. This trend shows that our digital era is not just confined to data behind screens and keyboards but is moving towards a cyber-physical world through sensors, actuators and autonomous systems.

Therefore, digital transformation led to face novel attack vectors and exploitable vulnerabilities within interconnected digital ecosystems. This evolution brings complex challenges at the intersection of cybersecurity, system security, and operational safety, thereby expanding the scope and criticality of the cyber domain.

In this context, the European Union has built a comprehensive cybersecurity regulatory framework in order to secure the European digital environment. In this scenario, cybersecurity certification process aims to be a tool that allows vendors, service providers, and ICT stakeholders in general, to gain a cybersecurity assurance of their solutions in order to be widely adopted in several use cases. For our purpose the relevant regulation is the Cybersecurity Act [1] that concurs to the achievement of the European objective in creating an high level of cybersecurity, cyber resilience and trust in the European Union (EU) by setting out a framework for the creation of voluntary European cybersecurity certification

Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), February 09-13, 2026, Cagliari, IT

*Corresponding author.

†These authors contributed equally.

m.malacario@acn.gov.it (M. Malacario); s.persia@acn.gov.it (S. Persia); i.dipietro@acn.gov.it (I. Di Pietro)

systems for Information and Communications Technology (ICT) products, services, processes, and managed security services.

In this context, the first European cybersecurity certification system adopted by the European Union is the European Union Cybersecurity Certification Scheme on Common Criteria, EUCC [2], based on the well-known international cybersecurity standard known as "Common Criteria" [3] [4][5] [6] [7] and related Evaluation Methodology [8].

Common Criteria is a wide adopted standard recognized at international level and it is considered the evolution of the preliminary approaches developed during the 1980 by the American Department of Defence (DoD) named "Orange Book" [9] about cybersecurity aspects when they became essential to protect information processed and transmitted through interconnected devices, and to provide a certain level of assurance in the cybersecurity of products.

The EUCC is a cybersecurity system based on two different assurance level that the product under certification can reach: substantial and high.

During the certification process it is important to define the boundaries of the evaluation. This means that it is fundamental to clearly define the characteristics of the product under evaluation, such as the unique product version, its configuration and its security functions that will be included in the scope of the evaluation. These boundaries allow to define the so-called Target of Evaluation (TOE) in Common Criteria.

Typically, under international mutual recognition, cybersecurity certificates have a validity of five years. Unfortunately, the certificate is valid for the specific TOE. It means that it is valid for a specific version of the product configured in a specific way. Any change occurred to the TOE, formally, impacts the certificate and its validity (e.g. functional evolutions, security patches, etc.) and then the issued certificate needs to be revised accordingly.

These constraints are clearly not in line with the rapid evolution of ICT, and for this reason the EUCC system stressed the "Assurance Continuity" that aims to define a process to maintain the validity of the certificate following the natural evolution of a certified product. Hence, the maintenance process of a certificate is an onerous endeavour that involves the Certification Body that issued the certificate, the laboratory that carried out the evaluation (named ITSEF - Information Technology Security Evaluation Facility) and the certificate holder/developer of the product.

Several initiatives, in both industrial and academic domains, have been performed to search solutions to optimize processes, with the scope to enhance their cost-effectiveness [10] and optimize the certification process by providing an incremental approach of the certification following the evolution of a system. In [11] authors proposed a lightweight and flexible incremental certification process, with DevSecOps (Development, Security, and Operations) practices, to automate evidence gathering in Assurance Continuity process as much as possible. This approach significantly accelerates and reduces the cost of gathering evaluation evidence, speeding up the process of certificate maintenance.

Aligned with previous contributions, but addressing the challenge from a different point of view, this paper proposes an approach that aims to reduce the effort required by the "Assurance Continuity" process providing a novel solution for certificate maintenance process optimization useful to permit a wider adoption of the EUCC in the next future.

Following the intuition of a possible correlation between these two "frameworks", explored by [12], the proposed approach is based on the Common Criteria Attack Potential concept, that is the "measure of the effort needed to exploit a vulnerability in a target of evaluation (TOE)" [4], by correlating it with CVSS score that "provides a way to capture the principal characteristics of a vulnerability and produce a numerical score" [13].

In this context, our work wants to analyse the problem by considering the TOE resistance against an attacker with a defined attack potential, by leveraging international framework for vulnerability classification, such as CVSS score, to automate the process of attack potential calculation starting from CVSS score of published CVEs.

The paper is organized as follows: a brief introduction of the TOE resistance, attack potential concepts and vulnerability analysis process are firstly carried out in the remainder of this section. In Section 2 and Section 3, the main concepts of the correlation of Attack Potential with CVSS and our approach are

respectively described in detail. Finally, in Section 4, conclusions are presented.

1.1. The concept of TOE resistance against an attacker with a defined attack potential

In Common Criteria evaluations, there are two main types of requirements:

- **Security Functional Requirements (SFRs)** are used to define the characteristics of the security functions of a product, such as the presence of an access control policy, the definition of the rules for enforcing that access control policy, etc. The SFR catalogue is listed in Common Criteria – Part 2 [4];
- **Security Assurance Requirements (SARs)** are used to verify whether the SFRs, defined for the TOE, are met in the whole life-cycle process. The SAR classes are divided in: ADV for the development; AGD for the guidance; ALC for the Life-Cycle; ATE for the testing phase; AVA for the vulnerability analysis. AVA is more relevant for our approach because this class has the scope to verify whether the TOE is resistant to attacks assuming a specific Attack Potential of an attacker (explained in detail in the following section 2.1). The catalogue of SAR is defined in Common Criteria – Part 3 [5].

AVA_VAN is structured in five different levels, from AVA_VAN.1 to AVA_VAN.5, and according to the Common Criteria, they classify the attack potential as:

- AVA_VAN.1 and AVA_VAN.2 capability to resist to an attack potential up to basic;
- AVA_VAN.3 capability to resist to an attack potential up to enhanced-basic;
- AVA_VAN.4 capability to resist to an attack potential up to moderate;
- AVA_VAN.5 capability to resist to an attack potential up to high.

EUCC, as already mentioned, simplifies the mapping according to:

- EUCC certificates at assurance level 'substantial' correspond to certificates that cover AVA_VAN level 1 or 2;
- EUCC certificates at assurance level 'high' correspond to certificates that cover AVA_VAN level 3, 4 or 5.

Hence, if an evaluation is done with an AVA_VAN.4 level, it means that the evaluator will verify that the TOE under test is resistant to attacks up to a moderate level according to the attack potential levels. It means that, if, during the evaluation process, an identified vulnerability requires a higher-level attack potential to be exploited, i.e. high, it will be considered residual.

In other words, its presence will be considered acceptable during the evaluation, and it will not impact the issuance of the certificate.

The concept is similar to the treatment and the acceptance of a residual risk. We remind that the Common Criteria standard does not consider risks level, but it relies on attack potentials, as furtherly analysed in [14]. Furthermore, in the definition of attack potential, the Common Criteria standard does not consider the impact due to the exploitation of a vulnerability, that is assumed in every case at maximum level. It means that the "residual vulnerability" concept does not include impact consideration.

The correspondence among vulnerability component, TOE resistance, and residual vulnerabilities is defined in [8] as shown in Table 1.

Before moving on, it is necessary to present the vulnerability analysis process showing where correlation between Attack Potential and the CVSS score of a CVE could act as a game-changing factor.

Table 1
Vulnerability, TOE resistance and Residual Vulnerability [8]

EUCC Level	Vulnerability	Basic	Enhanced Basic	Moderate	High	Beyond High
Substantial	AVA_VAN.1	Not residual	Residual	Residual	Residual	Residual
	AVA_VAN.2	Not residual	Residual	Residual	Residual	Residual
High	AVA_VAN.3	Not residual	Not residual	Residual	Residual	Residual
	AVA_VAN.4	Not residual	Not residual	Not residual	Residual	Residual
	AVA_VAN.5	Not residual	Not residual	Not residual	Not residual	Residual

1.2. The vulnerability analysis process

Vulnerability analysis is a fundamental phase in the evaluation activities based on Common Criteria standard. However, as explained in [15], the vulnerability analysis activity is not rigorous and the [8] is too generic, abstract and subjective. Our work is also intended to limit the subjectivity in the CVE analysis during the vulnerability analysis process that is presented in the following steps:

1. Evaluators investigate for possible vulnerabilities by collecting information relevant to the TOE from mailing lists, security forums, databases of public vulnerabilities (i.e. CVEs), outputs of functional tests carried out during the evaluation, TOE evidences, and their experience.

2. The collected data in step 1 leads to analyse possible attack scenarios. For each potential vulnerability analysed, applicability evaluation is needed.

3. If a vulnerability is deemed to be applicable, its exploitability needs to be evaluated. At this step, the evaluator shall calculate the Attack Potential related to the potential vulnerability, and the evaluator can realize that its exploitation may require a higher level than the one considered for the ongoing evaluation. So, he/she marks it as residual.

4. For the vulnerabilities with Attack Potential below the one indicated in the AVA_VAN level selected for the evaluation, evaluators need to check whether they are exploitable or not. If the vulnerability can be exploited, the Attack Potential calculation needs to be updated in order to double check if it is residual or not. If the value of the Attack Potential is lower, the vulnerability compromises the certificate emission, and thus mitigation activities from certificate holder/developer must be put in place.

The above-mentioned process is complex and time-consuming. For this reason, especially for the step 3, the possibility to use the CVSS score from the residual evaluation of a vulnerability becomes critical. CVSS is used for giving an estimation of the vulnerability severity through evaluating some exploitability and impact-depending parameters [13].

This framework was chosen due to its diffusion in the world. The [16] shows that about 300.000 CVE records have been published. The National Vulnerability Dashboard [17] highlights that about 180.000 CVE have been scored with CVE version 3.1. During 2024, about 40.704 CVEs have been published, each with its CVSS score [18]. Recent initiatives in Europe follow this approach [19].

According the EUCC, for each vulnerability applicable to a certified product, the certificate holder should initiate an assurance continuity process aimed to assess its applicability, its exploitability and its residuality through the Attack Potential calculation. According to the requirements of the EUCC scheme [2], steps from 1 to 4 presented above should therefore be applied during the Assurance Continuity (namely re-assessment process) for each vulnerability potentially applicable to a certified product. This process is time consuming for the main actors involved in the certificate management process: the Certification Body that is responsible for certificate issuance, Certificate Holder/Developer as owner of the certified product, and the testing laboratory ITSEF.

The definition of an automatic tool that is able to calculate the resulting Attack Potential starting from the CVSS score of a CVE would therefore allow an optimization of time/cost management. It will allow the certification actors to quickly classify all those vulnerabilities as residual or not.

Some studies, such as [20], propose the prioritization of vulnerability mitigation by relying only on the CVSS. Actually, CVSS focuses mainly on impact score of a vulnerability and does not provide adequate mechanisms for risk owners to make informed decisions regarding the risk.

Our approach will allow risk owners to prioritize the management of all those vulnerabilities, by establishing, with the usage of the correlation of CVSS score with attack potential, a risk acceptance level. This is done by the classification of a vulnerability as residual (that means risk acceptable) or not. This is the basis of our approach that can be structured in the following phases:

- **Phase A "Correlation":** definition of a correlation between Attack Potential and CVSS score [21].
- **Phase B "Analytical Approach":** definition of a corresponding analytical approach in order to develop a vulnerability management prioritization mechanism based on risk.

2. Analysis and correlation between Attack Potential and CVSS

In order to provide a novel analytical approach, it is fundamental to take into account the specification of the two main elements that will be analysed more in detail in the following sections:

- **Attack Potential** with the following main characteristics:
  - It is focused on the difficulty to exploit a vulnerability.
  - The metrics are focused on resources and competencies needed for successfully exploit a vulnerability.
  - It is a score used for evaluating the resistance of a product to attacks.
- **CVSS** with the following main characteristics:
  - It is focused on the severity of a vulnerability.
  - The metrics are focused on the impact and attack complexity.
  - It is used for determining the consequences of a vulnerability on a product.

The details of each element are reported in the following subsection.

2.1. Attack Potential

The Attack Potential is based on five factors defined in the Common Evaluation Methodology [8], each factor can assume the values shown in Table 2. The factors are:

- **Elapsed Time (ET)**: it represents the time taken to identify and exploit a vulnerability by an attacker. The exploitation phase should consider the time to develop an attack and time to execute the attack.
- **Expertise (Exp)**: this factor represents the specialist technical expertise required to the attacker. It can be considered as the level of knowledge pertaining to IT fundamental principles, product categories, and attack methodologies.
- **Knowledge of the TOE (KTOE)**: this parameter refers to the specific knowledge of the product under evaluation (i.e. TOE) in terms of architectural specification, source code, etc. It excludes any 'sensitive' information related to its specific configuration when deployed, such as user passwords.

Table 2
Values for Attack Potential factors according to CEM methodology [8]

Attack Potential factor	Qualitative Value	Quantitative Value
Elapsed Time	<= one day <= one week <= two weeks <= one months <= three months <= four months <= five mounths <= six mounths > six mounths	[0:19]
Expertise	Layman Proficeint Expert Multi Expers	[0:11]
Knowledge of TOE	Public Restricted Sensitive Critical	[0:11]
Window of Opportunity	Unnecessary/Unlimited Access Easy Moderate Difficulty None	[0:10] attack path is not exploitable
Equipment	Standard Specialised Bespoke Multiple bespoke	[0:9]

- **Window of Opportunity (WoO)**: it is a complex factor that represents the available time to access the TOE for performing the attack. In other words, the factor tries to model the scenarios where the interface, or the function, used for executing the attack is intermittently available (e.g., due to scheduled tasks such as cron jobs). On the other hand, this factor models the attackers' constraint of remaining undetected during the vulnerability exploitation (e.g. before an active monitoring system detects the attempted compromise or that the TOE implements Tamper-resistance mechanisms in order to prevent unauthorized access to sensitive information stored within the TOE such as key zeroization).
- **Equipment (Equip)**: refers to the equipment required to identify or exploit a vulnerability.

Note that, in Table 2, for each Attack Potential Factor depicted, according to the possible Qualitative Value assumed, the related Quantitative Value is a value that falls in the corresponding range. The correspondence between Qualitative Value and Quantitative Value is established by CEM methodology [8].

Hence, in order to provide an objective measure, CEM [8] provides a formula for computing this value:

$$AttackPotential = ET + Exp + KTOE + WoO + Equip \tag{1}$$

The equation (1) establishes the attack potential level needed by an attacker to exploit a defined vulnerability.

Table 3
Correspondence between values, attack potential levels meets assurance components and failure components [8].

Attack Potential	Quantitative values	AVA_VAN.1	AVA_VAN.2	AVA_VAN.3	AVA_VAN.4	AVA_VAN.5
Basic	[0:9]	Fail	Fail	Fail	Fail	Fail
Enached Basic	[0:13]	Meet	Meet	Fail	Fail	Fail
Moderate	[14:19]	Meet	Meet	Meet	Fail	Fail
High	[20:24]	Meet	Meet	Meet	Meet	Fail
Beyong High	[25:57]	Meet	Meet	Meet	Meet	Meet

In Table 3 the correspondence between values resulting from (1) and Attack Potential levels, with respectively meets assurance components and failure components, is depicted. These values will constitute key element for our proposed analytic approach described in Section 3.

2.2. Common Vulnerability Scoring System (CVSS)

CVSS 3.1 is based on three main metric groups that are [13]:

- The **Base** metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments.
  - The **Exploitability** metrics reflect the ease and technical means by which the vulnerability can be exploited.
  - The **Impact** metrics reflect the direct consequence of a successful exploit.
- The **Temporal** metric group reflects the characteristics of a vulnerability that may change over time but not across user environments. For example, the presence of a simple-to-use exploit kit would increase the CVSS score, while the creation of an official patch would decrease it.
- The **Environmental** metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment (e.g. presence of security controls which may mitigate some or all consequences of a successful attack).

Each metric group is composed of several metrics. For our analysis, we considered the metrics belonging to "Exploitability" and "Temporal" groups, as described in the following:

- **Attack Vector (AV)**: the context in which vulnerability exploitation is possible.
- **Attack Complexity (AC)**: the conditions beyond the attacker's control that must exist to exploit the vulnerability. (e.g. it may require the collection of more information about the target).
- **Privileges Required (PR)**: level of privileges an attacker must possess in order to successfully exploit the vulnerability.
- **User Interaction (UI)**: the requirement for a human user, other than the attacker, to participate in the successful compromise of the vulnerable component.
- **Scope**: the possibility offered by a vulnerability to move, through its exploitation, to another security domain, guarded by a different security authority, i.e., a mechanism that implements access control having some effect on a set of computer resources.

Table 4
Possible values of Exploitability Vector factors [13].

Factor	Value
Attack Vector (AV)	
Network	0,85
Adjacent	0,62
Local	0,55
Physical	0,2
Attack Complexity (AC)	
Low	0,77
High	0,44
Privileges Required (PR)	
None	0,85
Low (Scope unchanged)	0,62
Low (Scope changed)	0,68
High (Scope unchanged)	0,27
High (Scope changed)	0,5
User Interaction (UI)	
None	0,85
Required	0,62

- **Exploit Code Maturity (ECM)**: the likelihood of the vulnerability being attacked, it is typically based on the current state of exploit techniques, exploit code availability, or active, “in-the-wild” exploitation.

Hence the CVSS scheme defines values that each factor can be assumed during the evaluation phase. As an exemplary case, Table 4 shows the correspondence among the exploitability factors, the “Exploitability Vector" factors and corresponding values.

The equation to calculate the exploitability vector is:

$$exploitability = 8,22 \times AV \times AC \times PR \times UI \tag{2}$$

Note that, the metric “Exploit Code Maturity” is not included in (2). Anyway, this metric is a useful parameter for the attack potential correlation as reported in the following section.

2.3. Correlation between Attack Potential and CVSS

Starting from the definition of Attack Potential and CVSS, Table 5 has been built, listing possible correlations between the Attack Potential and CVSS factors. For each correspondence, a rationale is presented.

3. Proposed Analytic Approach

3.1. Assumption and hypotheses

The considerations made in the previous section led to consider a possible analytical approach. Based on Table 5 mapping is possible to build the system of equations in (3).

Table 5
Correlation between Attack Potential and CVSS Exploitability Vector factors

Attack Potential	CVSS metrics	Rationale
Elapsed Time		For a public vulnerability the elapsed time for identification can be considered as 0, as the vulnerability has been already identified.
	Exploit Code Maturity	Exploit Code Maturity is strictly related to the development of an attack method in the Elapsed Time factor (e.g. the highest value, High, corresponds to the minimum value, 0, for the development of an attack).
	Attack Vector	Attack Vector is strictly related to the exploitation factor. Time required for exploiting a vulnerability from the network is different from an exploitation that requires physical access.
Knowledge of the TOE	Exploit Code Maturity	Exploit Code Maturity is inversely proportional to the knowledge of the TOE: the higher the ECM, the lower the knowledge of the TOE that is needed by an attacker.
	Attack Complexity	Attack complexity: it is directly proportional to the knowledge of the TOE the higher the attack complexity, the higher the knowledge of the TOE that is needed by an attacker.
Expertise	Exploit Code Maturity	Exploit Code Maturity: it is inversely proportional to the specialist expertise required (i.e., if a proof-of-concept is public, the expertise required for its applicability is lower).
	Attack Complexity	Attack complexity is directly proportional to the expertise required for performing an attack. The higher the attack complexity, the higher the specialist expertise required.
Window of Opportunity		No direct mapping seems practicable, as the TOE operational environment should be known, however:
	Attack Vector	Attack vector is a parameter that influences the windows of opportunity (probably the exploitation from network has a higher window of opportunity w.r.t. a physical attack).
	User Interaction	User interaction: it is inversely proportional to the Window of opportunity.
	Privileges Required	Privileges required: the acquisition of higher privileges increments the time required for accessing the TOE.
Equipment	Attack Complexity	Attack complexity: for more complex attacks more resources should be required.
	Exploit Code Maturity	Exploit Code Maturity is strictly related to the need of develop an exploit (similar approach to what presented in Elapsed Time)

$$\begin{cases} ElapsedTime = f(AttackVector_1), f^{-1}(ExploitCodeMaturity_1) \\ KnoweledgeOfTOE = f(AttackComplexity_1), f^{-1}(ExploitCodeMaturity_1) \\ SpecialistExpertise = f(ArrackComplexity_2), f^{-}1(ExploitCodeMaturity_2) \\ WindowOfOpportunity = f(AttcakVector_2), f^{-1}(PrivilegesRequired_1), f(UserIntercation_1) \\ ITHWSoftwareEquopment = f(AttackComplexity_3), f^{-1}(ExploitCodeMaturity_3) \end{cases} \tag{3}$$

Actually, the system is not trivial to solve due to the number of variables with respect to the number of equations. It is possible to simplify the problem by introducing the following assumptions:

a. we discard the search for the optimum (i.e., a solution for the above equation system).

b. we search for heuristic solutions: the Exploitability Vector function is not an Attack Potential number, rather an Attack Potential level (i.e., basic, enhanced-basic, etc., instead of a range of integer values).

c. we do not consider beyond-high values of Attack Potential, as the top AVA_VAN component, i.e., AVA_VAN.5, takes into account a high Attack Potential at most, and it is therefore desirable that an ITSEF laboratory always analyses CVEs with such an attack potential without excluding such vulnerabilities *a priori*.

a), and b) assumptions lead to simplify the Exploitability Vector function to estimate the Attack Potential as:

$$AttackPotential = f(ExploitabilityVector) \tag{4}$$

Further simplification is obtained by assuming that our approach does not search for the exact correspondence between the numerical value of the Attack Potential and the corresponding Exploitability Vector function as reported in Figure 3. According to the c) assumption, we only consider the Attack Potential basic, enhanced-basic, moderate, high with a range of suitable value equal to

$$[0,\ 24]$$

. By these considerations the equation (4) can be simplified as:

$$y = f(x)\ where\ y \equiv [AP_{LEVEL}]\ and\ x \equiv ExploitabilityVector \tag{5}$$

Two possible values of x are:

- $a = 0,121090464$ is the minimum value of the Exploitability Vector by applying its formula to the minimum values presented in 4;
- $b = 3,887042775$ is the maximum value of the Exploitability Vector by applying its formula to the minimum values presented in 4.

We can observe that the Attack Potential and Exploitability Vector are inversely proportional quantities due to the fact that a vulnerability is highly exploitable, as the effort needed is lower.
This intuition is very clear if we focus on a specific factor of CVSS score: the "attack complexity". The exploitability vector experiments higher values when the attack complexity is lower.
Hence, the boundaries of the function can be calculated as follows:

$$f(a) = 24\ (HIGH) \tag{6}$$

(6) means that the minimum value of the exploitability vector corresponds to the maximum value of the High Attack Potential equal to 24:

$$f(b) = 0\ (BASIC) \tag{7}$$

In the same way, it is possible to assume that the maximum value of the exploitability vector corresponds to the minimum value of the Basic Attack Potential: 0.
The analytical approach aims to find the following:

$$Find\ x_1 = f^{-1}(19),\ x_2 = f^{-1}(13),\ x_3 = f^{-1}(9),\ x_1, x_2, x_3 \in [a, b]\ such\ that$$

$$f(x) = \begin{cases} HIGH,\ if\ x \in [a, x_1) \\ MODERATE,\ if\ x \in [x_1, x_2) \\ ENAHNCED\ BASIC,\ if\ x \in [x_2, x_3) \\ BASIC,\ if\ x \in [x_3, b) \end{cases} \tag{8}$$

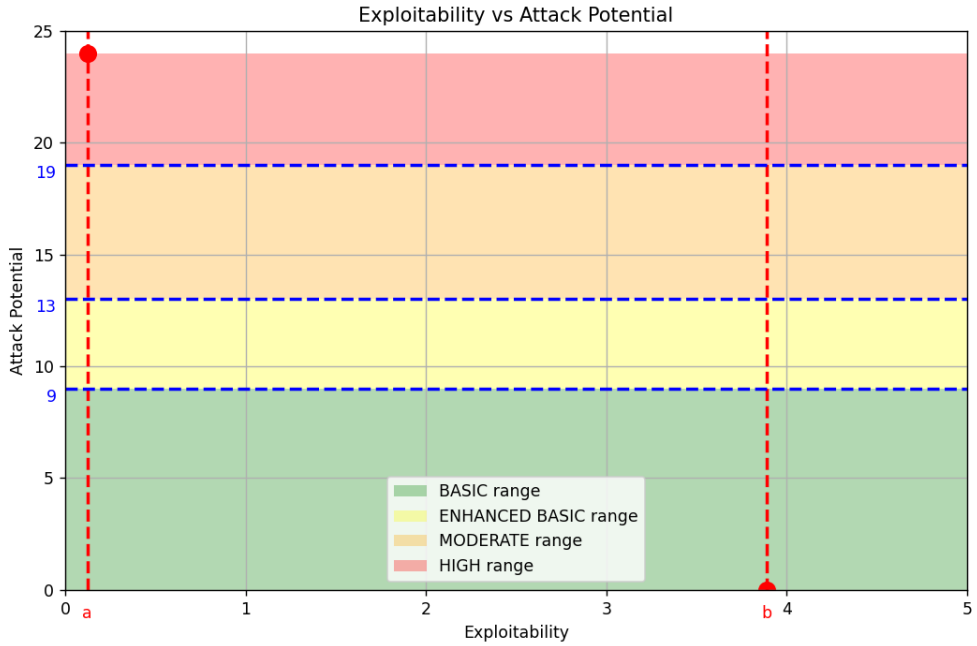

Figure 1: Exploitability vs. Attack Potential.

From a visual point of view, it is possible to draw a plane with the exploitability vector values on the $x - axis$ and the Attack Potential values on the $y - axis$ as in Figure 1.

We simplified the resolution of the problem by applying a heuristic approach, based on the following steps:

- Collection of a reliable CVE dataset, with CVSS score and Attack Potential computed for each vulnerability.
- Plot of all curves passing through extremes.
- Measurement of the error for each curve with respect to the dataset.

The details of the above step are described in the following subsections.

3.2. The Dataset

The CVE dataset taken into account for the validation of our analytical approach has been selected by considering samples from a subset of CVE discovered by the internal ITSEF of ACN - the National Agency of Cybersecurity of Italy – on several ICT devices. It is noted that the ACN ITSEF discovers about 40 vulnerabilities per year [22].

For the dataset definition two main principles have been targeted:

- **Uniform data**: because CVEs can be discovered by different evaluators employed in the ITSEF laboratory, the aspect could influence the affordability of the CVEs due to different interpretations of the parameters of the Attack Potential and CVSS by different evaluators. To resolve this issue, CVEs discovered by the same evaluator have been taken into account.
- **Static bias avoidance**: to avoid static bias, vulnerabilities have been selected starting from a uniform distribution of attack potential and CVSS values.

Figure 2 shows results of our approach by considering 20 vulnerabilities, where it is possible to note some verticals in the figure due to the fact that the exploitability vector can assume only 65 different values in accordance with the equation (2), and the inverse proportionality with the attack potential is also confirmed.

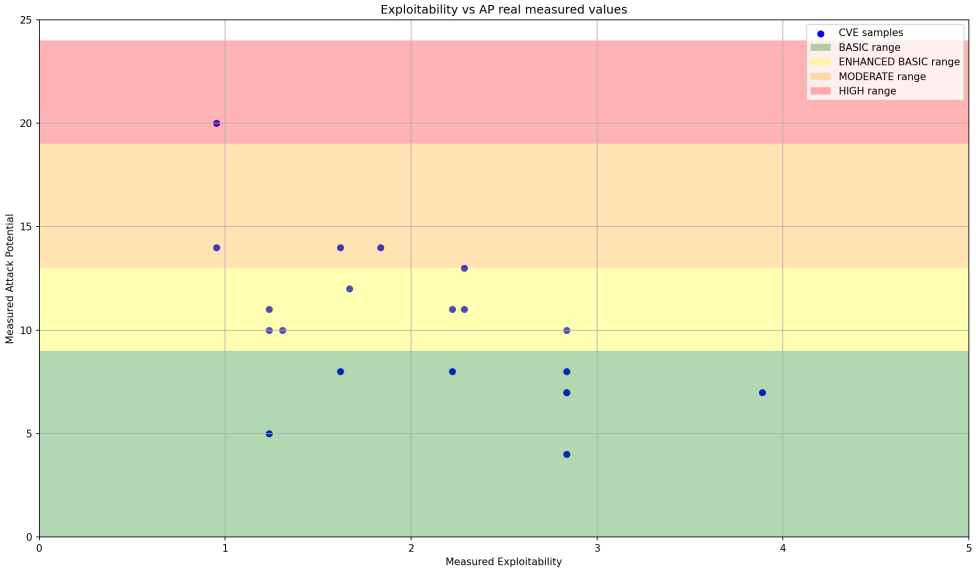

Figure 2: Dataset distribution

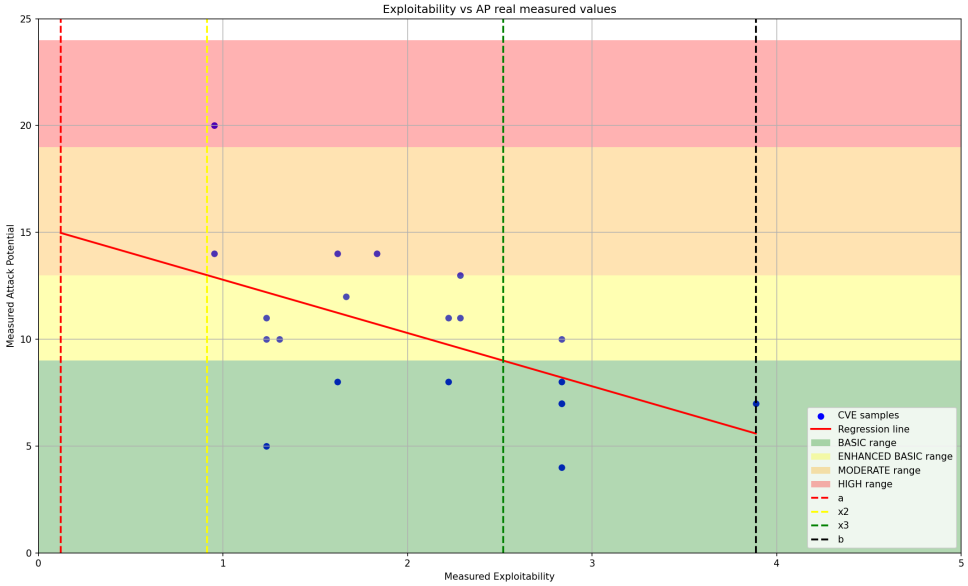

Figure 3: First attempt (statistical): regression line

3.3. Problem resolution

To resolve the problem by an analytical point of view some interpolation functions have been considered starting from the values available in the prepared dataset. Two different cases, CASE A and CASE B have been reported and explained in detail.

CASE A - the linear function (6) is taken into account (statistical regression line):

$$y \approx -2.49x \ + 15.28 \tag{9}$$

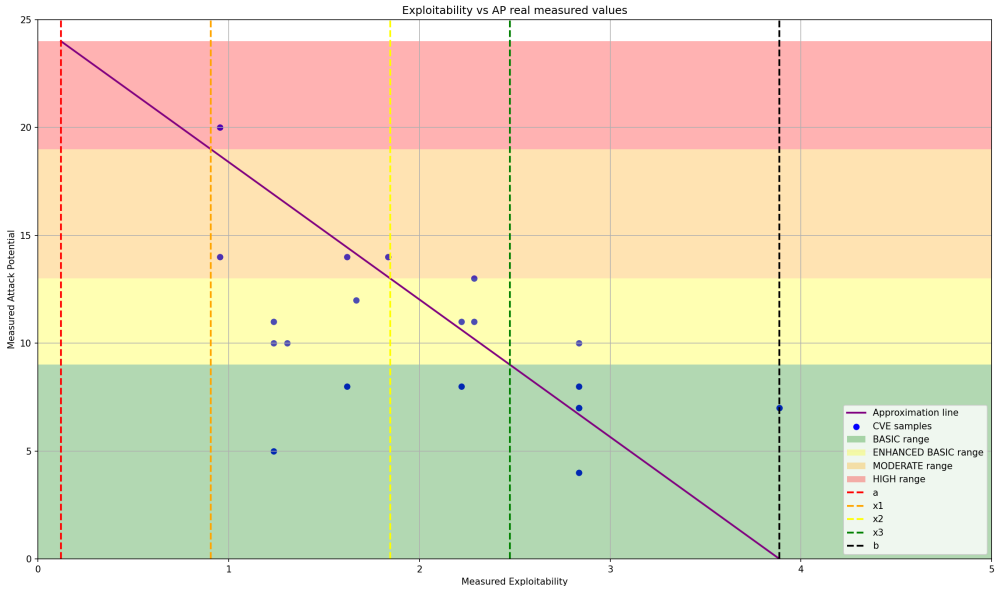

Figure 4: Second attempt (analytical): line through extreme.

For this case the estimation appears not good enough (see Figure 3) due to the following observation:

- Estimation to $HIGH$ attack potential is never possible (x_1 is negative)
- Extremes are not coherent with the assumptions
- Results: 12 matches out of 20
  - 4 errors by excess [1] of 1
  - 1 error by excess[1] of 2
  - 3 errors by defect of 1: they can be considered less severe because an overestimation of Attack Potential leads to false positive. In the worst case the evaluator check a vulnerability that potentially will be classified as residual.

CASE B - A more detailed linear function has been taken into account:

$$\begin{cases} 24 = ma + q \\ 0 = mb + q \end{cases} \tag{10}$$

$$y = mx + q \approx -6.37x + 24.77$$

The estimation appears better than Case A (see Figure 4) due to the following observation:

- Extremes are coherent with the assumptions
- Estimation to HIGH is possible

The results can be summarized as:

- Result: 12 matches out of 20 (**but less severe**)
  - 4 errors by excess[1] of 1

[1] where $excess$ means that the understimation of Attack Potential leads to the presence of false negative.

- 2 errors by defect of 1 (less severe)
- 2 errors by defect of 2 (less severe)

By the observations of the results, we can conclude that is needed to find a better interpolation function, and it can be reached by acquiring a larger dataset to evaluate the right functions. In particular, future works could explore a Machine Learning approach by considering different dataset by distinguishing "training" dataset and "control" dataset.

The possibility to include the EPSS [23] for "adjusting" the curves could improve the results.

We remind that, the EPSS is an open framework for assessing vulnerability threats, that is the probability that a vulnerability will be exploited in the wild within the first 12 months after public disclosure. In this context, from a larger point of view the EPSS could be used in a useful way for calculating the risk value of a vulnerability helping the prioritization:

$$Risk\ = CVSS(as\ Impact\ value)\ \cdot EPSS(as\ Probability\ value) \tag{11}$$

In this way, risk evaluation can support monitoring of public vulnerability for defining priority or "not residual" vulnerabilities in patching or assurance continuity activities, and the EPSS could be considered as possible substitute factor for exploit code maturity parameter in CVSS.

Furthermore, it is noticed that, for minimizing the subjective interpretation of CVSS and Attack Potential parameters, it is desirable the definition of a suitable "User Guide" for CVSS and Attack Potential parameters definition. This may enhance consistency in judgements by different evaluators in ITSEFs.

In a similar way the Attack Potential definition could be further revised in order to include additional metrics that could help in the Attack Potential estimations in a more objective manner in the future.

4. Conclusions and Future work

Due to the rapidly evolving landscape of the emerging technologies, the need for effective tools to strengthen the cybersecurity posture of the digital ecosystem has become critical.

Cybersecurity certification may act as cornerstone for providing assurance in product security, thereby fostering trust and promoting systemic resilience within the market.

Achieving a good balance between the need to obtain the assurance through a cybersecurity certification and the need to maintain IT product update is increasingly critical in today's dynamic technological landscape. The Assurance Continuity mechanism within the EUCC certification system plays a pivotal role in this context. Consequently, it becomes essential to develop cost-effective frameworks that support product evolution while ensuring timely prioritization and remediation of newly discovered vulnerabilities in order to maintain the validity of the cybersecurity certification.

The proposed approach in this work aims to provide a possible automation framework to correlate the CVSS score of CVE to the corresponding Attack Potential. A possible analytic approach has been proposed, where the 60% of CVSS score has been correctly correlated with the corresponding attack potential level in the best-case situation, while the remaining 20% has been underestimated, and 20%, overestimated. Future work will be focused on the possibility to reduce the percentage of wrong estimations evaluating the possibility to introduce further metrics such as EPSS for adjusting the model.

Acknowledgments

We want thank Gaetano Cavarretta, Massimiliano Orazi, Gianluca Roascio, Pierpaolo Santucci and Lorenzo Zamburru for their help in in the early stages of the idea and the model definition.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] EU, Regulation (EU) 2019/881 of the European Parlament and of the Council of 17 April 2029 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repeakung Regulation (EU) No 526/2013 (Cybersecurity Act), EU, 2019.

[2] EU, Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC), EU, 2024.

[3] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, volume CCMB-2022-11-001, 2022.

[4] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, volume CCMB-2022-11-002, 2022.

[5] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, volume CCMB-2022-11-003, 2022.

[6] Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities, volume CCMB-2022-11-004, 2022.

[7] Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements, volume CCMB-2022-11-005, 2022.

[8] Common Methodology for Information Technology Security Evaluation Evaluation methodology, volume CCMB-2022-11-006, 2022.

[9] NCS, Department of defense trusted computer system evaluation criteria," Techical Report CSC-STD-001-83, NCS Association, 1985.

[10] A. Morgagni, P. Massonet, S. Dupont, G. Jeremy, Towards incremental safety and security requirements co-certification, 2020, pp. 79–84. doi:10.1109/EuroSPW51379.2020.00020.

[11] S. Dupont, G. Ginis, M. Malacario, C. Porretti, N. Maunero, C. Ponsard, P. Massonet, Incremental common criteria certification processes using DevSecOps practices, 2021, pp. 12–23. doi:10.1109/EuroSPW54576.2021.00009.

[12] T. Boswell, Attack Potential:Using it Properly and Evolving it for the future, 2008.

[13] First, Common vulnerability scoring system version 3.1, specification document, revision 1, 2019. URL: https://www.first.org/cvss/.

[14] K. Beckers, I. Côté, S. Fenz, D. Hatebur, M. Heisel, A Structured Comparison of Security Standards, 2014, pp. 1–34. doi:10.1007/978-3-319-07452-8_1.

[15] C. Zhou, S. Ramacciotti, Common criteria: Its limitations and advice on improvement, Information Systems Security Association ISSA (2011) 24–28.

[16] CVE, cve^{TM} program mission., 2025. URL: https://www.cve.org.

[17] NIST, Nvd dashboard., 2025. URL: https://nvd.nist.gov/general/nvd-dashboard.

[18] Éireann Leverett, The 2024 vulnerability forecast: Year in review., 2025. URL: https://www.first.org/blog/20250106-Vulnerability-Forecast-Year-in-Review.

[19] ENISA, European union vulnerability database., 2025. URL: https://euvd.enisa.europa.eu.

[20] L. Miranda, L. Senos, D. Menasché, G. Srivastava, A. Kocheturov, E. Lovat, A. Ramchandran, T. Limmer, A product-oriented assessment of vulnerability severity through NVD CVSS scores, 2025, pp. 238–242. doi:10.1109/ICNC64010.2025.10994117.

[21] M. Malacario, G. Cavarretta, M. Orazi, S. Persia, L. Zamburru, Cvss as a tool for attack potential calculation, in: Proceedings of the International Common Criteria Conference, Doha, Qatar, 2024.

[22] ACN, Agenzia per la Cybersicurezza Nazionale, Relazione annuale al parlamento, 2024.

[23] J. Jacobs, s. Romanosky, B. Edwards, M. Roytman, I. Adjerid, Exploit prediction scoring system (EPSS), Digital Threats: Research and Practice 2 (2021). doi:10.1145/3436242.