Common Vulnerability Scoring System 3.1

(CVSS 3.1)

YD Chiang

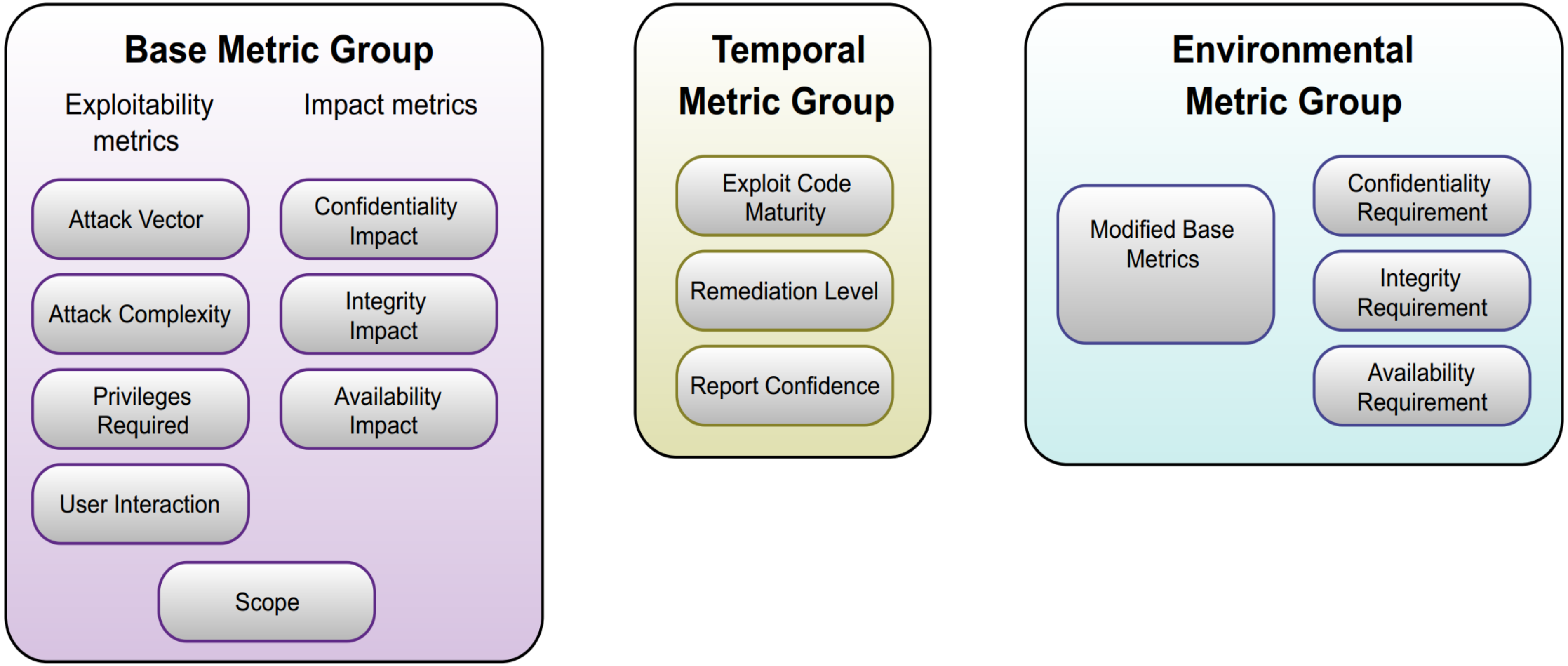
2023/12/16

Introduction

- The Common Vulnerability Scoring System (CVSS) captures the principal technical characteristics of software, hardware and firmware vulnerabilities.
- CVSS is composed of three metric groups: **Base**, **Temporal**, and **Environmental**.
  - Base: Reflects the severity of a vulnerability according to its intrinsic characteristics which are constant over time and assumes the reasonable worst-case impact across different deployed environments.
  - Temporal: Adjusts the Base severity of a vulnerability based on factors that change over time, such as the availability of exploit code.
  - Environmental: Adjusts the Base and Temporal severities to a specific computing environment. They consider factors such as the presence of mitigations in that environment.

Metrics

- CVSS is composed of three metric groups: Base, Temporal, and Environmental.
  - Base Group: Exploitability (可利用性) + Impact (影響性)



Base Metric Group

Exploitability metrics

Attack Vector

Attack Complexity

Privileges Required

User Interaction

Impact metrics

Confidentiality Impact

Integrity Impact

Availability Impact

Scope

Temporal Metric Group

Exploit Code Maturity

Remediation Level

Report Confidence

Environmental Metric Group

Modified Base Metrics

Confidentiality Requirement

Integrity Requirement

Availability Requirement

Base Metrics

- Exploitability Metrics
  - **Attack Vector (AV)**: Reflects the context by which vulnerability exploitation is possible. This metric value will be larger the more remote. The assumption is that the number of potential attackers for a vulnerability that could be exploited from across a network is larger than the number of potential attackers that could exploit a vulnerability requiring physical access to a device.

Metric Value	Description	Example
Network (N)	Such a vulnerability is often termed “remotely exploitable” and can be thought of as an attack being exploitable at the protocol level one or more network hops away (e.g., across one or more routers).	DDos
Adjacent (A)	The attack is limited at the protocol level to a logically adjacent topology. This can mean an attack must be launched from the same shared physical (e.g., Bluetooth or IEEE 802.11) or logical (e.g., local IP subnet) network, or from within a secure or otherwise limited administrative domain(e.g., VPN).	ARP (IPv4) or neighbor discovery (IPv6) flood leading.
Local (L)	The vulnerable component is not bound to the network stack and the attacker’s path is via read/write/execute capabilities. The attacker exploits the vulnerability by accessing the target system locally or relies on User Interaction by another person to perform actions.	
Physical (P)	The attack requires the attacker to physically touch or manipulate the vulnerable component.	Evil maid attack, USB DMA

Base Metrics

- Exploitability Metrics
  - **Attack Complexity (AC)**: Describes the conditions beyond the attacker’s control that must exist to exploit the vulnerability. Such conditions may require the collection of more information about the target, or computational exceptions.

Metric Value	Description
Low (L)	Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable success when attacking the vulnerable component.
High (H)	A successful attack depends on conditions beyond the attacker‘s control. A successful attack cannot be accomplished at will but requires the attacker to invest in some measurable amount of effort in preparation or execution against the vulnerable component before a successful attack can be expected. • The attacker must gather knowledge about the environment in which the vulnerable target/component exists. (系統設定、序號編碼方式、共用的密碼) • The attacker must prepare the target environment to improve exploit reliability. (繞過漏洞緩解措施) • The attacker must inject themselves into the logical network path between the target and the resource requested by the victim in order to read and/or modify network communications. (利用中間人攻擊技術)

Base Metrics

- Exploitability Metrics
  - **Privileges Required (PR)**: Describes the level of privileges an attacker must possess before successfully exploiting the vulnerability.

Metric Value	Description
None (N)	The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.
Low (L)	The attacker requires privileges that provide basic user capabilities that could normally affect only settings and files owned by a user. An attacker with Low privileges has the ability to access only non-sensitive resources.
High (H)	The attacker requires privileges that provide significant (e.g., administrative) control over the vulnerable component allowing access to component-wide settings and files.

Base Metrics

- Exploitability Metrics
  - **User Interaction (UI)**: This metric determines whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner.

Metric Value	Description
None (N)	The vulnerable system can be exploited without interaction from any user.
Required (R)	Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited. For example, a successful exploit may only be possible during the installation of an application by a system administrator.

Base Metrics

- Impact Metrics
  - **Confidentiality (C)**: Confidentiality refers to limiting information access and disclosure to only authorized users. This metric measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability.

Metric Value	Description
High (H)	There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact. For example, an attacker steals the administrator's password, or private encryption keys of a web server.
Low (L)	There is some loss of confidentiality. Access to some restricted information is obtained, but the attacker does not have control over what information is obtained, or the amount or kind of loss is limited. The information disclosure does not cause a direct, serious loss to the impacted component.
None (N)	There is no loss of confidentiality within the impacted component.

Base Metrics

- Impact Metrics
  - **Integrity (I)**: Integrity refers to the trustworthiness and veracity of information. This metric measures the impact to integrity of a successfully exploited vulnerability.

Metric Value	Description
High (H)	There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
Low (L)	Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is limited. The data modification does not have a direct, serious impact on the impacted component.
None (N)	There is no loss of integrity within the impacted component.

Base Metrics

- Impact Metrics
  - **Availability (A)**: Availability refers to the accessibility of information resources. This metric refers to the loss of availability of the impacted component itself, such as a networked service (e.g., web, database, email).

Metric Value	Description
High (H)	There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component. The attacker has the ability to deny some availability, but the loss of availability presents a direct, serious consequence to the impacted component (e.g., the attacker cannot disrupt existing connections, but can prevent new connections; the attacker can repeatedly exploit a vulnerability that, in each instance of a successful attack, leaks only small amount of memory, but after repeated exploitation causes a service to become completely unavailable).
Low (L)	Performance is reduced or there are interruptions in resource availability. The resources in the impacted component are either partially available all of the time, or fully available only some of the time, but overall, there is no direct, serious consequence to the impacted component.
None (N)	There is no impact to availability within the impacted component.

Base Metrics

- Scope (S)
  - If a vulnerability in a vulnerable component can affect a component which is in a different security scope than the vulnerable component, a Scope change occurs.
  - The security scope of a component encompasses other components that provide functionality solely to that component, even if these other components have their own security authority.

Metric Value	Description
Unchanged (U)	An exploited vulnerability can only affect resources managed by the same security authority.
Changed (C)	An exploited vulnerability can affect resources beyond the security scope managed by the security authority of the vulnerable component.

Temporal Metrics

- **Exploit Code Maturity (E)**: This metric measures the likelihood of the vulnerability being attacked. The exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently.

Metric Value	Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Temporal Score, i.e., it has the same effect on scoring as assigning High.
High (H)	Functional autonomous code exists, or no exploit is required, and details are widely available. Exploit code works in every situation, or is actively being delivered via an autonomous agent (such as a worm or virus). Network-connected systems are likely to encounter scanning or exploitation attempts. Exploit development has reached the level of reliable, widely available, easy-to-use automated tools.
Functional (F)	Functional exploit code is available. The code works in most situations where the vulnerability exists.
Proof-of-Concept (P)	Proof-of-concept exploit code is available, or an attack demonstration is not practical for most systems. The code or technique is not functional in all situations and may require substantial modification by a skilled attacker.
Unproven (U)	No exploit code is available, or an exploit is theoretical.

Temporal Metrics

- **Remediation Level (RL)**: The Remediation Level of a vulnerability is an important factor for prioritization. The typical vulnerability is unpatched when initially published. Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued.

Metric Value	Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Temporal Score, i.e., it has the same effect on scoring as assigning Unavailable.
Unavailable (U)	There is either no solution available or it is impossible to apply.
Workaround (W)	There is an unofficial, non-vendor solution available. In some cases, users of the affected technology will create a patch of their own or provide steps to work around or otherwise mitigate the vulnerability.
Temporary Fix (T)	There is an official but temporary fix available. This includes instances where the vendor issues a temporary hotfix, tool, or workaround.
Official Fix (O)	A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available.

Temporal Metrics

- **Report Confidence (RC)**: This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. The urgency of a vulnerability is higher when a vulnerability is known to exist with certainty. This metric also suggests the level of technical knowledge available to would-be attackers.

Metric Value	Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Temporal Score, i.e., it has the same effect on scoring as assigning Confirmed.
Confirmed (C)	Detailed reports exist, or functional reproduction is possible (functional exploits may provide this). Source code is available to independently verify the assertions of the research, or the author or vendor of the affected code has confirmed the presence of the vulnerability.
Reasonable (R)	Significant details are published, but researchers either do not have full confidence in the root cause, or do not have access to source code to fully confirm all of the interactions that may lead to the result. Reasonable confidence exists, however, that the bug is reproducible and at least one impact is able to be verified (proof-of-concept exploits may provide this). An example is a detailed write-up of research into a vulnerability with an explanation (possibly obfuscated or “left as an exercise to the reader”) that gives assurances on how to reproduce the results.
Unknown (U)	There are reports of impacts that indicate a vulnerability is present. The reports indicate that the cause of the vulnerability is unknown, or reports may differ on the cause or impacts of the vulnerability. Reporters are uncertain of the true nature of the vulnerability, and there is little confidence in the validity of the reports or whether a static Base Score can be applied given the differences described. An example is a bug report which notes that an intermittent but non-reproducible crash occurs, with evidence of memory corruption suggesting that denial of service, or possible more serious impacts, may result.

Environmental Metrics

- **Security Requirements (CR, IR, AR)**: These metrics enable the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user's organization, measured in terms of Confidentiality, Integrity, and Availability. The full effect on the environmental score is determined by the corresponding Modified Base Impact metrics.
- For example, the Modified Confidentiality impact (MC) metric has increased weight if the Confidentiality Requirement (CR) is High. Likewise, the Modified Confidentiality impact metric has decreased weight if the Confidentiality Requirement is Low.

Metric Value	Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score, i.e., it has the same effect on scoring as assigning Medium.
High (H)	Loss of [Confidentiality | Integrity | Availability] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
Medium (M)	Loss of [Confidentiality | Integrity | Availability] is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
Low (L)	Loss of [Confidentiality | Integrity | Availability] is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).

Environmental Metrics

- **Modified Base Metrics**: These metrics enable the analyst to override individual Base metrics based on specific characteristics of a user’s environment. Characteristics that affect Exploitability, Scope, or Impact can be reflected via an appropriately modified Environmental Score.
- The intent of this metric is to define the mitigations in place for a given environment. It is acceptable to use the modified metrics to represent situations that increase the Base Score.

Modified Base Metric	Corresponding Values
Modified Attack Vector (MAV)	The same values as the corresponding Base Metric (see Base Metrics above), as well as Not Defined (the default).
Modified Attack Complexity (MAC)	
Modified Privileges Required (MPR)	
Modified User Interaction (MUI)	
Modified Scope (MS)	
Modified Confidentiality (MC)	
Modified Integrity (MI)	
Modified Availability (MA)	

Qualitative Severity Rating Scale

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10

Vector String

- The CVSS v3.1 vector string is a text representation of a set of CVSS metrics. It is commonly used to record or transfer CVSS metric information in a concise form.
- A vector string should contain metrics in the order shown in the table, though other orderings are valid.
- All Base metrics must be included in a vector string. Temporal and Environmental metrics are optional, and omitted metrics are considered to have the value of Not Defined (X).
- For example, a vulnerability with Base metric values of "Attack Vector: Network, Attack Complexity: Low, Privileges Required: High, User Interaction: None, Scope: Unchanged, Confidentiality: Low, Integrity: Low, Availability: None" and no specified Temporal or Environmental metrics would produce the following vector:
CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N
- The same example with the addition of "Exploitability: Functional, Remediation Level: Not Defined" and with the metrics in a non-preferred ordering would produce the following vector:
CVSS:3.1/S:U/AV:N/AC:L/PR:H/UI:N/C:L/I:L/A:N/E:F/RL:X

Metric Group	Metric Name (and Abbreviated Form)	Possible Values	Mandatory?
Base	Attack Vector (AV)	[N,A,L,P]	Yes
	Attack Complexity (AC)	[L,H]	Yes
	Privileges Required (PR)	[N,L,H]	Yes
	User Interaction (UI)	[N,R]	Yes
	Scope (S)	[U,C]	Yes
	Confidentiality (C)	[H,L,N]	Yes
	Integrity (I)	[H,L,N]	Yes
	Availability (A)	[H,L,N]	Yes
Temporal	Exploit Code Maturity (E)	[X,H,F,P,U]	No
	Remediation Level (RL)	[X,U,W,T,O]	No
	Report Confidence (RC)	[X,C,R,U]	No
Environmental	Confidentiality Requirement (CR)	[X,H,M,L]	No
	Integrity Requirement (IR)	[X,H,M,L]	No
	Availability Requirement (AR)	[X,H,M,L]	No
	Modified Attack Vector (MAV)	[X,N,A,L,P]	No
	Modified Attack Complexity (MAC)	[X,L,H]	No
	Modified Privileges Required (MPR)	[X,N,L,H]	No
	Modified User Interaction (MUI)	[X,N,R]	No
	Modified Scope (MS)	[X,U,C]	No
	Modified Confidentiality (MC)	[X,N,L,H]	No
	Modified Integrity (MI)	[X,N,L,H]	No
	Modified Availability (MA)	[X,N,L,H]	No

CVSS v3.1 Equations

- The CVSS v3.1 equations are defined in the sub-sections below. They rely on helper functions defined as follows:
  - Minimum returns the smaller of its two arguments.
  - Roundup returns the smallest number, specified to 1 decimal place, that is equal to or higher than its input. For example, Roundup (4.02) returns 4.1; and Roundup (4.00) returns 4.0. To ensure consistent results across programming languages and hardware, see Appendix A for advice to Implementers on avoiding small inaccuracies introduced in some floating point implementations.

CVSS v3.1 Equations

- Base Metrics Equations: The Base Score formula depends on sub-formulas for Impact Sub-Score (ISS), Impact, and Exploitability, all of which are defined below:

ISS =	**1 - [(1 - Confidentiality) × (1 - Integrity) × (1 - Availability)]**
Impact =	
If Scope is Unchanged	$6.42 \times \text{ISS}$
If Scope is Changed	$7.52 \times (\text{ISS} - 0.029) - 3.25 \times (\text{ISS} - 0.02)^{15}$
Exploitability =	$8.22 \times \text{AttackVector} \times \text{AttackComplexity} \times \text{PrivilegesRequired} \times \text{UserInteraction}$
BaseScore =	
If Impact <= 0	0, *else*
If Scope is Unchanged	Roundup (Minimum [(Impact + Exploitability), 10])
If Scope is Changed	Roundup (Minimum [1.08 × (Impact + Exploitability), 10])

CVSS v3.1 Equations

- Temporal Metrics Equations

TemporalScore = Roundup (BaseScore × ExploitCodeMaturity × RemediationLevel × ReportConfidence)

CVSS v3.1 Equations

- Environmental Metrics Equations

MISS =	**Minimum (1 - [(1 - ConfidentialityRequirement × ModifiedConfidentiality) × (1 - IntegrityRequirement × ModifiedIntegrity) × (1 - AvailabilityRequirement × ModifiedAvailability)], 0.915)**
ModifiedImpact =	
If ModifiedScope is Unchanged	6.42 × MISS
If ModifiedScope is Changed	$7.52 \times (\mathrm{MISS} - 0.029) - 3.25 \times (\mathrm{MISS} \times 0.9731 - 0.02)^{13}$

ModifiedExploitability =	8.22 × ModifiedAttackVector × ModifiedAttackComplexity × ModifiedPrivilegesRequired × ModifiedUserInteraction

CVSS v3.1 Equations

- Environmental Metrics Equations

EnvironmentalScore =

If ModifiedImpact <= 0	0, *else*
If ModifiedScope is Unchanged	Roundup (Roundup [Minimum ([ModifiedImpact + ModifiedExploitability], 10)] × ExploitCodeMaturity × RemediationLevel × ReportConfidence)
If ModifiedScope is Changed	Roundup (Roundup [Minimum (1.08 × [ModifiedImpact + ModifiedExploitability], 10)] × ExploitCodeMaturity × RemediationLevel × ReportConfidence)

CVSS v3.1 Equations

- Metric Values

Metric	Metric Value	Numerical Value
Attack Vector / Modified Attack Vector	Network	0.85
	Adjacent	0.62
	Local	0.55
	Physical	0.2
Attack Complexity / Modified Attack Complexity	Low	0.77
	High	0.44
Privileges Required / Modified Privileges Required	None	0.85
	Low	0.62 (or 0.68 if Scope / Modified Scope is Changed)
	High	0.27 (or 0.5 if Scope / Modified Scope is Changed)
User Interaction / Modified User Interaction	None	0.85
	Required	0.62
Confidentiality / Integrity / Availability / Modified Confidentiality / Modified Integrity / Modified Availability	High	0.56
	Low	0.22
	None	0
Exploit Code Maturity	Not Defined	1
	High	1
	Functional	0.97
	Proof of Concept	0.94
	Unproven	0.91
Remediation Level	Not Defined	1
	Unavailable	1
	Workaround	0.97
	Temporary Fix	0.96
	Official Fix	0.95
Report Confidence	Not Defined	1
	Confirmed	1
	Reasonable	0.96
	Unknown	0.92
Confidentiality Requirement / Integrity Requirement / Availability Requirement	Not Defined	1
	High	1.5
	Medium	1
	Low	0.5