New Score Formula

I. Overview of the CVSS 3.1 standard:

1. The process of assessing security vulnerabilities using CVSS:

   A vulnerability assessed using the CVSS 3.0 standard must adhere to the following criteria.

   Attack Vector – This metric is determined by how much access is needed to take advantage of a vulnerability. A lower score necessitates an attack to occur at a physical on-premise location, whereas a higher score indicates that an exploit can be carried out remotely from outside the organization.

   Attack Complexity – This metric is based on factors like middle-man attacks and key theft that are beyond the control of the attacker. The attacker must exert additional effort beyond the scope of the cyberattack in order to receive a higher score.

   Required Privileges – The attacker's privileges to take advantage of a vulnerability are the basis for this metric. Whereas a lower score indicates little to no privileges required, a higher score indicates the level of administration privileges required to carry out an attack.

   User Interaction – This metric measures whether an attacker can successfully carry out the attack by enlisting the help of an unaware or willing victim. A higher score indicates that no further involvement is required.

   Scope – The number of components required to exploit a vulnerability serves as the basis for scope metrics. A deeper backend system attack may result from a single exploit attack, hence the higher score.

   Confidentiality – The amount of data that the attacker has access to is the basis for this metric. The attacker can access the most data if their score is higher; if it's lower, no data can be accessed.

   Integrity – Based on the attacker's capacity to change data on the exploited system, this metric is calculated. If the attacker completely or significantly modifies the data, the score is high.

   Availability – This metric is based on the damage caused to the system after an exploit. A higher score indicates that an attack will make the system inaccessible to authorized users.

2. Detailed information about vectors:

- **Attack Vector (AV):**

  - Network: 0.85
  - Adjacent: 0.62
  - Local: 0.55
  - Physical: 0.2

Value	Description
Network (N)	Attackers are said to be "remotely exploitable" if they can access a vulnerability only through OSI layer 3.
Adjacent (A)	Attacker can only use a shared physical network to exploit vulnerability.
Local (L)	Attacker either relies on user interaction or locally exploits the vulnerability.
Physical (P)	The attacker must physically contact or exert control over the vulnerable component.

- **Attack Complexity (AC):**
  - Low: 0.77
  - High: 0.44

Value	Description
Low (L)	Attacker can take advantage of the vulnerable component more than once.
High (H)	To carry out a successful attack on the vulnerable component, the attacker must be better prepared.

- **Privileges Required (PR):**
  - None: 0.85
  - Low: 0.62
  - High: 0.27

Value	Description
None (N)	The attacker doesn't require settings or file access to launch an attack. Unauthorized attacker.
Low (L)	Attacker needs privileges to modify settings and files that they hold most frequently. The attacker

	has little authority.
High (H)	The attacker needs access to files and settings that impact the entire component, giving them complete control.

- **User Interaction (UI):**
  - None: 0.85
  - Requirement: 0.62

Value	Description
None (N)	Vulnerabilities can be taken advantage of without the user's involvement.
Required (R)	Only after taking some sort of action is the user able to exploit the vulnerability.

- **Scope (S):**
  - Unchanged.
  - Changed.

Value	Description
Unchanged (U)	The identical component is both vulnerable and impacted. The same authority is in charge of the resources involved.
Changed (C)	Differences exist between the vulnerable component and the component that is impacted. Resource control is not exercised by the same authority.

- **Confidentiality (C):**
  - None: 0.56
  - Low: 0.22
  - High: 0

Value	Description
High (H)	Due to complete confidentiality loss, the attacker has access to all resources of the damaged component.

Low (L)	The restricted information that is accessed is not under the attacker's control. There is some confidentiality loss.
None (N)	No compromise of privacy.

- **Integrity (I):**
  - None: 0.56
  - Low: 0.22
  - High: 0

Value	Description
High (H)	complete lack of protection or integrity. Aattacker can change any file.
Low (L)	Attacker can change a file, but they have no control over the results.
None (N)	No loss of integrity.

- **Availability (A):**
  - None: 0.56
  - Low: 0.22
  - High: 0

Value	Description
High (H)	An attacker can prevent the impacted component's resources from being fully accessed. Complete loss of accessibility.
Low (L)	Attacker is unable to fully deny. Resources, whether partial or whole, are only accessible for a limited time.
None (N)	No loss of availability.

- **Conversion table:**

0.0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High

9.0-10	Critical

3. 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 × ISS

If Scope is Changed: 7.52 × (ISS - 0.029) - 3.25 × (ISS - 0.02)15

Exploitability = 8.22 × AttackVector × AttackComplexity × PrivilegesRequired × 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])

II. CVSS Scores of some security vulnerabilities:

Name	Severity	CVSS Score	CVSS Vector
SQL Injection	High	8.6	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Name	Severity	CVSS Score	CVSS Vector
LFI (Local File Inclusion)	High	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Name	Severity	CVSS Score	CVSS Vector
XSS	Medium	5.4	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

Name	Severity	CVSS Score	CVSS Vector
Path Traversal	High	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Name	Severity	CVSS Score	CVSS Vector
IDOR	Medium	6.5	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

Name	Severity	CVSS Score	CVSS Vector

File Upload	High	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

III. Scanner's scoring formula:

Website safety rate = [1 - (Total vulnerabilities score/ Total original score)] * 100

Each flaw will have an original score of 10. If an error is detected, subtract the error's score from 10, add up the total, divide by the total score and multiply by 100.

Ex: A website has 10 vulnerabilities, including 5 errors with a score of 8.6; 7.5; 3.2; 9.8; 4.5. It will be calculated as follows:

[1 - (8.6 + 7.5 + 3.2 + 9.8 + 4.5)/ 100] * 100 = 66.4

And then convert according to the conversion table:

39 - 0	Critical
69 - 40	High
89 - 70	Medium
99 - 90	Low
100	None

Beyondsecurity. (2023, October 21). CVSS Explained.

https://www.beyondsecurity.com/blog/cvss-explained

First. (2023, October 21). Common Vulnerability Scoring System v3.1: Specification Document.

https://www.first.org/cvss/v3.1/specification-document