DISCLAIMER

Il materiale contenuto nel drive è stato raccolto e richiesto tramite autorizzazione ai ragazzi frequentanti il corso di studi di Informatica dell'Università degli Studi di Salerno. Gli appunti e gli esercizi nascono da un uso e consumo degli autori che li hanno creati e risistemati per tanto non ci assumiamo la responsabilità di eventuali mancanze o difetti all'interno del materiale pubblicato.

Il materiale sarà modificato aggiungendo il logo dell'associazione, in tal caso questo possa recare problemi ad alcuni autori di materiale pubblicato, tale persona può contattarci in privato ed elimineremo o modificheremo il materiale in base alle sue preferenze.

Ringraziamo eventuali segnalazioni di errori così da poter modificare e fornire il miglior materiale possibile a supporto degli studenti.

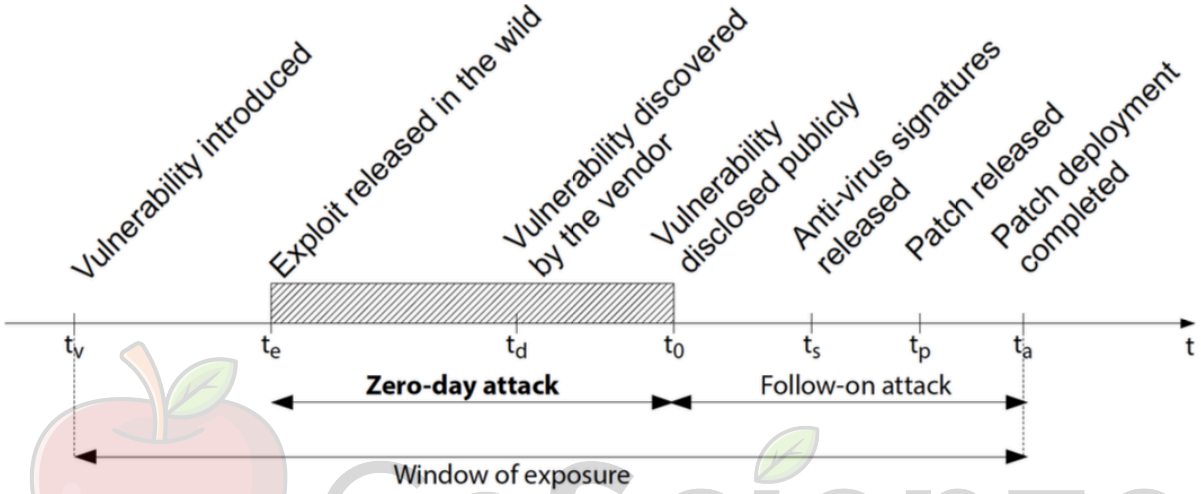
CoScienze
Associazione

Alfonso Cannavale

CATALOGAZIONE DELLE VULNERABILITÀ

Per **vulnerabilità** si intende una debolezza presente, comprensibile e sfruttabile da un attaccante. Il *ciclo di vita* di una vulnerabilità ha le seguenti fasi:

1. ***(t_v)*** Rilascio di un software, o di una nuova versione, che presenta una vulnerabilità;
2. ***(t_e)*** Scoperta della vulnerabilità da parte di un attaccante, rilascio di un exploit per sfruttare la vulnerabilità non notificando il fornitore;
3. ***(t_d)*** Scoperta della vulnerabilità da parte del fornitore, o tramite segnalazione, viene notificato il problema;
4. ***(t_0)*** Divulgazione della vulnerabilità al pubblico;
5. ***(t_s)*** Rilevazione dell'exploit da parte degli antivirus, aggiornando i sistemi di protezione in modo da poter rilevare l'exploit;
6. ***(t_p)*** Rilascio di una patch da parte del venditore;
7. ***(t_a)*** Mitigazione dell'exploit su tutti i sistemi.



- Nell'intervallo $[t_e, t_0]$ la vulnerabilità è stata sfruttata nell'*oscurità* (la vulnerabilità è sfruttata all'insaputa di tutti) -> l'attacco effettuato nel periodo $[t_e, t_0]$ viene detto **zero-day attack**.
- Nell'intervallo $[t_0, t_a]$ la vulnerabilità è stata sfruttata pubblicamente -> l'attacco effettuato nel periodo $[t_0, t_a]$ avviene in presenza della conoscenza pubblica della vulnerabilità ed è chiamato **follow-on attack**.
- L'intervallo $[t_v, t_a]$ costituisce la finestra di esposizione della vulnerabilità.

Più vicini si è allo *zero-day*, più è probabile che un attacco al software abbia successo.

Catalogare le vulnerabilità

È importante tenere traccia delle vulnerabilità note perché fornisce agli utenti e agli sviluppatori informazioni cruciali per proteggere i propri sistemi e software. Ciò può essere fatto mediante:

- **Enumerazione**, ovvero costruzione di una tupla univoca per ciascuna vulnerabilità così composta: *(id, tipo di vulnerabilità, vettore di attacco, minaccia, exploit)*;
- **Catalogazione**, ovvero inserimento della tuple in un apposito archivio.

In passato, sono stati proposti diversi archivi indipendenti da diverse aziende creando problemi di duplicazione ed eterogeneità, infatti, nel 1998 una stessa vulnerabilità venne catalogata per 12 volte da team differenti.

Common Vulnerability Exposure (CVE)

Nel 1999 venne creato il **MITRE**, un ente no-profit, che ha introdotto un catalogo uniforme delle vulnerabilità chiamato **Common Vulnerability Exposures (CVE)**. Le vulnerabilità presenti nel CVE violano almeno una proprietà della triade CIA, inoltre esse sono identificate da una stringa univoca CVE-ANNO-NUMERO e sono descritte da una scheda esplicativa contenente: descrizione della vulnerabilità, link a pagine dettagliate (references) e data di creazione.

Common Vulnerability Scoring System

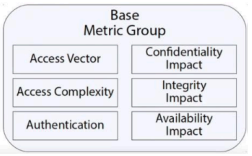
Il CVE enumera le vulnerabilità, ma *non ne misura l'impatto*, infatti non stabilisce quale tra le vulnerabilità debba essere gestita più urgentemente e come le vulnerabilità possano impattare su sistemi diversi. Per questo motivo è stato introdotto il **Common Vulnerability Scoring System (CVSS)**, che stima la gravità di ogni vulnerabilità e assegna ad ogni CVE id un punteggio da 0 a 10, dove 0 rappresenta un impatto nullo e 10 rappresenta un impatto critico. Ci sono due versioni del CVSS (v2 e v3), entrambe assegnano il punteggio in base a tre gruppi di metriche:

- *Base (base metric)*: Stimano la gravità della vulnerabilità, a prescindere da fattori temporali e ambientali rispondono alle seguenti domande: Qual è il vettore di attacco? Quanto è semplice sfruttare la vulnerabilità? Qual è l'impatto sulla triade delle proprietà CIA?
- *Temporali (temporal metric)*: Stimano la gravità della vulnerabilità dal punto di vista temporale: È disponibile un exploit? È disponibile una patch?
- *Ambientali (environmental metric)*: Stimano la gravità della vulnerabilità dal punto di vista ambientale. Qual è la conseguenza di un exploit su persone e cose? Quanti sistemi sono vulnerabili?

Ad ogni metrica è associata una domanda a risposta multipla, ciascuna risposta fornisce un peso numerico e i singoli pesi sono poi aggregati in un risultato finale tramite una serie di formule.

BASE (BASE METRIC):

Stimano la gravità delle vulnerabilità, a prescindere da fattori temporali e ambientali.



La metrica ***Access Vector*** risponde alla domanda:

- *Tramite quale vettore di accesso può essere sfruttata la vulnerabilità?*

Valore	Descrizione	Punt.
Local (L)	L'attaccante deve avere accesso fisico/un account sul sistema.	0.395
Adjacent Network (A)	L'attaccante deve avere accesso al dominio di broadcast o di collisione del sistema.	0.646
Network (N)	L'interfaccia vulnerabile è al livello 3 o superiore della pila ISO/OSI.	1.0

La metrica ***Access Complexity*** risponde alla domanda:

- *Quanto è difficile sfruttare la vulnerabilità?*

Valore	Descrizione	Punt.
High (H)	Lo sfruttamento richiede condizioni particolari (corsa critica, tecniche di social engineering).	0.35
Medium (M)	Lo sfruttamento richiede alcune condizioni (ad es., configurazione non di default).	0.646
Low (L)	Lo sfruttamento non richiede nulla di particolare (funziona su sistemi standard).	1.0

La metrica ***Authentication*** risponde alla domanda:

- *Quante volte un attaccante si deve autenticare per sfruttare la vulnerabilità?*

Valore	Descrizione	Punt.
Multiple (M)	Lo sfruttamento richiede due o più autenticazioni (anche con le stesse credenziali).	0.45
Single (S)	Lo sfruttamento richiede una sola autenticazione.	0.56
None (N)	Lo sfruttamento non richiede alcuna forma di autenticazione.	0.704

La metrica ***Confidentiality Impact*** risponde alla domanda

- *Qual è l'impatto della vulnerabilità sulla confidenzialità del sistema?*

Valore	Descrizione	Punt.
None (N)	Non vi è impatto alcuno.	0.0
Partial (P)	É possibile divulgare solo un sotto-insieme dei dati offerti dal sistema.	0.275
Complete (C)	É possibile divulgare l'intero insieme dei dati offerti dal sistema.	0.660

La metrica ***Integrity Impact*** risponde alla domanda:

- *Qual è l'impatto della vulnerabilità sull'integrità del sistema?*

Valore	Descrizione	Punt.
None (N)	Non vi è impatto alcuno.	0.0
Partial (P)	É possibile modificare solo un sotto-insieme dei dati offerti dal sistema.	0.275
Complete (C)	É possibile modificare l'intero insieme dei dati offerti dal sistema.	0.660

La metrica ***Availability Impact*** risponde alla domanda:

- *Qual è l'impatto della vulnerabilità sulla disponibilità del sistema?*

Valore	Descrizione	Punt.
None (N)	Non vi è impatto alcuno.	0.0
Partial (P)	É possibile ridurre parzialmente le prestazioni e/o le funzioni offerte dal sistema.	0.275
Complete (C)	É possibile ridurre completamente le prestazioni e/o le funzioni offerte dal sistema.	0.660

Le risposte relative alle metriche base sono presentate sotto forma di stringa di testo, che viene chiamata ***vector string***, è formata da coppie di abbreviazioni ***mestrica:risposta*** separate dal carattere **/**. Esempio

AV:N/AC:L/Au:N/C:P/I:P/A:C

Viene dato un punteggio a questa stringa in base alle metriche delle tabelle, che verrà restituito il ***Punteggio Base***, ovvero la stima della gravità della vulnerabilità senza considerare fattori temporali ed ambientali.

$$Exploitability = 20 * AccessVector * AccessComplexity * Authentication$$

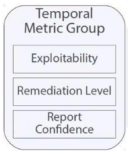
$$Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact))$$

$$f(Impact) = \begin{cases} 0 & if\ Impact = 0 \\ 1.176 & otherwise \end{cases}$$

$$BaseScore = roundTo1Decimal(((0.6 * Impact) + (0.4 * Exploitability) - 1.5) * f(Impact))$$

I punteggi associati alle altre due metriche sono opzionali e si calcolano nello stesso modo ma con questionari diversi. Esistono ***relazioni tra i punteggi***, infatti il punteggio *temporale* ingloba il *base* e quello *ambientale* ingloba il *temporale*. Pertanto, il punteggio *ambientale* è quello più generale possibile che ingloba i due precedenti.

TEMPORALI (TEMPORAL METRIC):
Stimano la gravità della vulnerabilità dal punto di vista temporale.



La metrica ***Exploitability*** risponde alla domanda:

- *Qual è lo stato attuale delle tecniche di sfruttamento della vulnerabilità?*

Valore	Descrizione	Punt.
Unproven (U)	L'exploit non è pubblico, oppure esiste in linea solo teorica.	0.85
Proof of Concept (P)	È disponibile una bozza dimostrativa (**Proof of Concept**, **PoC**). Richiede adattamenti non banali per funzionare.	0.9
Functional (F)	È disponibile un exploit funzionante nella maggioranza dei casi in cui la vulnerabilità è presente.	0.95
High (H)	La vulnerabilità può essere sfruttata in modo automatico (anche da worm e virus).	1.0
Not Defined (ND)	Si ignori tale punteggio.	1.0

La metrica ***Remediation Level*** risponde alla domanda:

- È presente un rimedio per mitigare la vulnerabilità?

Valore	Descrizione	Punt.
Official fix (O)	Il vendor mette a disposizione un rimedio ufficiale (patch, aggiornamento software).	0.87
Temporary fix (T)	Il vendor mette a disposizione un rimedio ufficiale, ma temporaneo.	0.90
Workaround (W)	Una terza parte (NON il vendor) mette a disposizione un rimedio non ufficiale.	0.95
Unavailable (U)	Non è disponibile un rimedio, o è impossibile applicare una soluzione suggerita.	1.0
Not Defined (ND)	Si ignori tale punteggio.	1.0

La metrica ***Report Confidence*** risponde alla domanda:

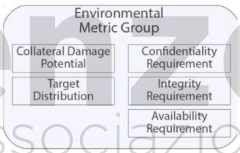
- *La vulnerabilità esiste veramente? È descritta in maniera credibile?*

Valore	Descrizione	Punt.
Unconfirmed (UC)	La vulnerabilità è divulgata da una singola fonte non confermata, o da più fonti in mutuo conflitto.	0.9
Uncorroborated (UR)	La vulnerabilità è divulgata da più fonti concordi. Può esistere un livello residuo di incertezza.	0.95
Confirmed (C)	La vulnerabilità è confermata dal vendor.	1.0
Not Defined (ND)	Si ignori tale punteggio.	1.0

Il ***Punteggio Temporale*** stima la gravità della vulnerabilità includendo il fattore temporale

$$TemporalScore = roundTo1\ Decimal\ (\ BaseScore * Exploitab * RemedLvl * ReportConf\ )$$

AMBIENTALI (ENVIRONEMENT METRIC):
Stimano la gravità della vulnerabilità dal punto di vista ambientale.



La metrica ***Collateral Damage Potential*** risponde alla domanda:

- *Qual è l'impatto della vulnerabilità sui sistemi fisici, sulle persone e sulle risorse finanziarie?*

Valore	Descrizione	Punt.
None (N)	Nessun impatto.	0
Low (L)	Danno fisico basso, perdita marginale di guadagno.	0.1
Low-Medium (LM)	Danno fisico ed economico moderato.	0.3
Medium-High (MH)	Danno fisico ed economico significativo.	0.4
High (H)	Danno fisico ed economico catastrofico.	0.5
Not Defined (ND)	Si ignori tale punteggio.	1.0

La metrica ***Target Distribution*** risponde alla domanda:

- *Quale percentuale di asset è soggetta alla vulnerabilità?*

Valore	Descrizione	Punt.
None (N)	Percentuale nulla.	0
Low (L)	1%-25% degli asset.	0.25
Medium (M)	26%-75% degli asset.	0.75
High (H)	76%-100% degli asset.	1.0
Not Defined (ND)	Si ignori tale punteggio.	1.0

La metrica ***Confidentiality Requirement*** risponde alla domanda:

- *Qual è l'impatto di una perdita di confidenzialità?*

Valore	Descrizione	Punt.
Low (L)	L'impatto è lieve.	0.5
Medium (M)	L'impatto è serio.	1.0
High (H)	L'impatto è catastrofico.	1.51
Not Defined (ND)	Si ignori tale punteggio.	1.0

La metrica ***Integrity Requirement*** risponde alla domanda:

- *Qual è l'impatto di una perdita di integrità?*

Valore	Descrizione	Punt.
Low (L)	L'impatto è lieve.	0.5
Medium (M)	L'impatto è serio.	1.0
High (H)	L'impatto è catastrofico.	1.51
Not Defined (ND)	Si ignori tale punteggio.	1.0

La metrica ***Availability Requirement*** risponde alla domanda:

- *Qual è l'impatto di una perdita di disponibilità?*

Valore	Descrizione	Punt.
Low (L)	L'impatto è lieve.	0.5
Medium (M)	L'impatto è serio.	1.0
High (H)	L'impatto è catastrofico.	1.51
Not Defined (ND)	Si ignori tale punteggio.	1.0

Il ***Punteggio Ambientale*** stima la gravità della vulnerabilità includendo il fattore ambientale

$$AdjImp = min(10, 10.41 * (1 - (1 - ConfImp * ConfReq) * (1 - IntImp * IntReq) * (1 - AvImp * AvReq)))$$

$$AdjTemp = \text{punteggio Temporal ricalcolato con } AdjImp \text{ al posto di Impact}$$

$$EnvironmentalScore = roundTo1\ Decimal\ ((AdjTemp + (10 - AdjTemp) * CollatDamPot) * TargetDist)$$

Punteggio CVSS
I punteggi CVSS *base e temporali sono calcolati dai venditori di software*, mentre quello *ambientale è calcolato dagli amministratori delle infrastrutture*. Questi punteggi vengono utilizzati da chiunque abbia a che fare con il processo di gestione della sicurezza. Esiste un foglio di calcolo che, rispondendo alle domande, è possibile ottenere il punteggio.