

Incorporating Vulnerabilities into Risk Analysis

José A. Mañas

17.5.2010

Abstract

1	Introduction.....	1
2	Vulnerabilities.....	2
2.1	CPE	2
2.2	CVSS	2
2.3	CWE.....	3
3	PILAR.....	3
3.1	Assets	3
3.2	Threats.....	3
4	Annex A – CVSS.....	3
4.1	Short summary	4
5	Annex B - File formats	6
5.1	CPE: official dictionary	6
5.2	Vulnerabilities: xml format.....	6
5.3	Refinement of vulnerabilities: xml format.....	7
6	Annex C – Scripts	7

1 Introduction

This document is about vulnerabilities in the sense of CVE (Common Vulnerabilities and Exposures)

An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network.

CVE considers a mistake a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system (this excludes excluding entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system).

For CVE, a vulnerability is a state in a computing system (or set of systems) that either:

- allows an attacker to execute commands as another user
- allows an attacker to access data that is contrary to the specified access restrictions for that data
- allows an attacker to pose as another entity
- allows an attacker to conduct a denial of service

Source: <http://cve.mitre.org/>

The paper describes how PILAR incorporates published information on vulnerabilities to derive just-in-time estimates of risk on information systems.

2 Vulnerabilities

According to CVE, a vulnerability is reported with a number of items that characterize it:

- id:
a unique key
- summary:
a description in natural language.
- vulnerability configuration:
a formula for computers describing the combination(s) of hardware and software that is(are) subject to the vulnerability; uses CPE.
- vulnerability software list:
a list of software items that are subject to the vulnerability; uses CPE.
- cvss (common vulnerability scoring system):
metrics to qualify the vulnerability; see annex.
- cwe (common weakness enumeration):
a reference to a type of weakness in software.

2.1 CPE

CPE™ is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

Further information may be found at <http://cpe.mitre.org/>

2.2 CVSS

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems.

Further information may be found at <http://nvd.nist.gov/cvss.cfm>

See Annex A.

2.3 CWE

International in scope and free for public use, CWE™ provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Further information may be found at <http://cpe.mitre.org/>.

3 PILAR

Currently, PILAR incorporates information from CVE:

- using the unique id to reference the published vulnerability
- using CPE to associate vulnerabilities to assets
- using CVSS Metrics to derive a potential likelihood of occurrence
- using CVSS Impact Metrics to derive a degradation (consequences of occurrence of a threat)

3.1 Assets

PILAR enables the association of CPE identifiers to assets.

3.2 Threats

More precisely, the following values are used to derive an estimate of likelihood:

- access vector
- access complexity
- authentication
- exploitability
- remediation level
- report confidence

And the following values are used to derive an estimate of degradation on security dimension C, I, or A:

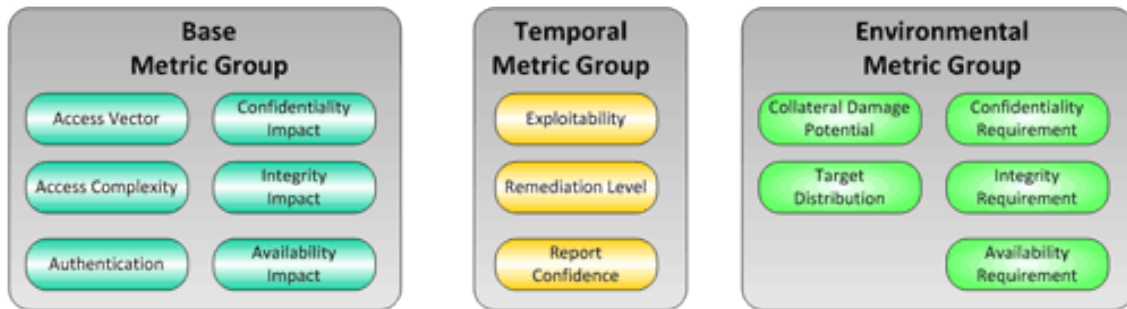
- impact on C, I, or A
- exploitability
- remediation level
- report confidence

Users may override these estimations, and provide explicit values for likelihood or degradation.

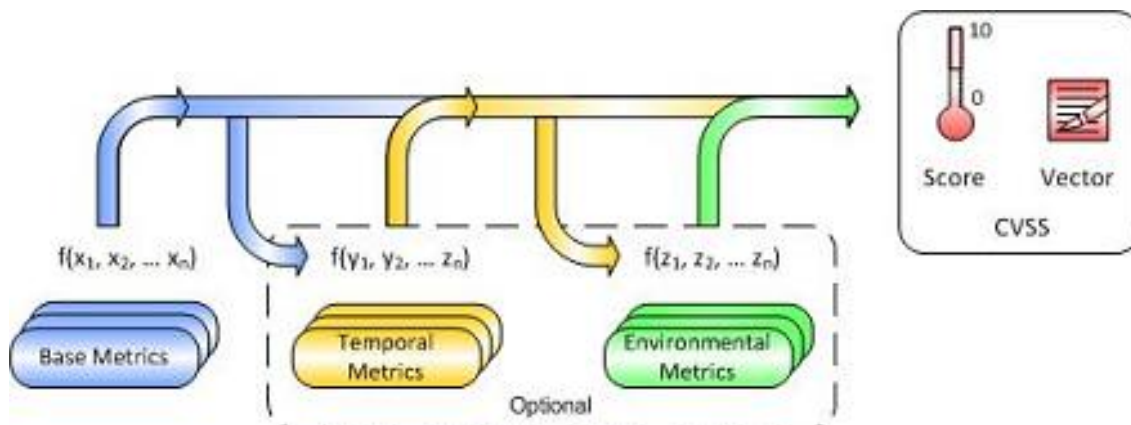
4 Annex A – CVSS

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of 3 groups: Base, Temporal and Environmental. Each group produces a

numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.



When the base metrics are assigned values, the base equation calculates a score ranging from 0 to 10, and a vector is created, as illustrated below.



4.1 Short summary

AV - Access Vector

This metric reflects how the vulnerability is exploited.

L - Local

A - Adjacent Network

N - Network

AC - Access Complexity

This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system.

H - High

M - Medium

L - Low

AU - Authentication

This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability.

M - Multiple

S - Single

N - None

C - Confidentiality Impact

This metric measures the impact on confidentiality of a successfully exploited vulnerability.

N - None

P - Partial

C - Complete

C - Integrity Impact

This metric measures the impact to integrity of a successfully exploited vulnerability.

N - None

P - Partial

C - Complete

C - Availability Impact

This metric measures the impact to availability of a successfully exploited vulnerability.

N - None

P - Partial

C - Complete

E - Exploitability

This metric measures the current state of exploit techniques or code availability.

U - Unproven

POC - Proof of Concept

F - Functional

H - High

ND - Not Defined

RL - Remediation Level

The remediation level of a vulnerability is an important factor for prioritization.

OF - Official Fix

TF – Temporary Fix

W – Workaround

U – Unavailable

ND – Not Defined

RC – Report Confidence

This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details.

UC – Unconfirmed

UR – Uncorroborated

C – Confirmed

ND – Not Defined

5 Annex B - File formats

PILAR reads several files to retrieve information about vulnerabilities and their application to the system under analysis.

5.1 CPE: official dictionary

See

<http://cpe.mitre.org/dictionary/index.html>

The schema is described in

http://cpe.mitre.org/files/cpe-dictionary_2.2.zip

The dictionary is updated from time to time. The official dictionary may be downloaded from

<http://nvd.nist.gov/cpe.cfm>

http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/official-cpe-dictionary_v2.2.xml

This dictionary is loaded by PILAR in order to assign CPE names to assets. Once loaded, PILAR remembers the associations, and there is no need to load every time.

5.2 Vulnerabilities: xml format

See

<http://nvd.nist.gov/download.cfm>

The schema is described in

http://nvd.nist.gov/schema/nvd-cve-feed_2.0.xsd

PILAR uses these feeds when searching for vulnerabilities associated to a CPE. Found vulnerabilities are assigned to those assets labelled with the CPE. PILAR loads CVSS values, that you may edit on screen, or update from a local updates file (see next section).

5.3 Refinement of vulnerabilities: xml format

```
file ::=
  <vulnerability-updates>
    { item }0+
  </vulnerability-updates>

item ::=
  <cve id="CVE-2008-7236"
    cpe= comma-separated list
    cvss= cvss full vector
    cvss_av= access vector
    cvss_ac= access complexity
    cvss_au= authentication
    cvss_c= confidentiality impact
    cvss_i= integrity impact
    cvss_a= availability impact
    cvss_e= exploitability
    cvss_rl= remediation level
    cvss_rc= report confidence
    freq= real value
    deg_c= percentage of degradation of confidentiality
    deg_i= ... integrity
    deg_a= ... availability
    deg_auth= ... authenticity
    deg_acc= ... accountability
  />
```

All attributes are optional, but "id".

The codes used in CVSS lines are those described along the paragraphs in Annex A.

Percentages are integer numbers in the range 0-100.

PILAR uses these values to repair values loaded from CVE feeds. If a value is not provided, PILAR keeps the original value.

6 Annex C – Scripts

The following orders extend scripts used in batch mode.

```
<search-vulnerabilities>
  /lib/vulnerabilities/cve.mitre.org/nvdcve-2.0-modified.xml
</search-vulnerabilities>

<update-vulnerabilities>
  /lib/vulnerabilities/cve.mitre.org/updates_2010-05-04.xml
</update-vulnerabilities>
```