

# Automated Software Vulnerability Management

## Table of Contents

1	Introduction.....	4
1.1	Software Vulnerability Management .....	4
2	Automated Vulnerability Management .....	5
2.1	System Components .....	5
2.2	System Work flow .....	5
3	Standards .....	6
3.1	SCAP .....	6
4	Alternatives to NVD Repository .....	7
5	Discussion .....	8
6	Conclusion .....	9

**Abstract.** Text of the summary of your article

## 1 Introduction

One of the main concerning area for most of organizations is information and software assets security which can be achieved by utilizing the software and network security techniques like firewall, but this is not sufficient to ensure the safety of the information assets due the continuous discovery of software vulnerabilities and put the organization's IT assets in risk of cyber attacks by adversary. Most of organization should be ware and updated about the open software vulnerabilities and perform the need actions like installing the corresponding patch if available, an such information about open vulnerabilities can be retrieved from repositories like National Vulnerability Database NVD. The manual processing of vulnerabilities data requires a quite amount of human resource and could be not affordable for all organizations that motivates for building an automated software vulnerabilities management systems which in general try to alert in organizations about the open vulnerabilities related to the organization's IT assets utilizing the data of on-line repositories such NVD, also another sources of data can be also used like the software vulnerability information provided on social media or blogs.

### 1.1 Software Vulnerability Management

The software Vulnerability Management concept can be defined as the process of identifying the related vulnerabilities for the software components inside the organization, the process requires firstly managing the inventory of organization's IT assets and periodic search for the related vulnerabilities, and in case of vulnerability discovery a certain action should be performed such alerting the administrators or trying to install the corresponding patch es to avoid possible threats based on those known vulnerabilities.

## **2 Automated Vulnerability Management**

### **2.1 System Components**

### **2.2 System Work flow**

### 3 Standards

This section introduces one of the most related standards for the software vulnerability management which is the Security Content Automation Protocol (SCAP) [1].

#### 3.1 SCAP

SCAP is a collection of open standards and enumerations related to software flaws and security configurations that allow the communication of that information, to support the automated vulnerability and security information management. It is provided and maintained by The U.S. National Institute of Standards and Technology (NIST) [2], and the large and public part of the SCAP content is the National Vulnerability Database (NVD) [3] that provides data feed for each SCAP standard which can be used free by the public security community, which also is managed by NIST. SCAP has gained adoption by most of the information security systems. The SCAP standards consist of different open standards and enumerations, and the following subset of them:

- Common Vulnerabilities and Exposures (CVE)
- Common Platform Enumeration (CPE)
- Common Configuration Enumeration (CCE)
- Common Vulnerability Scoring System (CVSS)

The CVE is the naming list of software flaws in security context, to allow identification of cyber-security vulnerabilities to ease the exchange of information about the cyber-security issues. The CVE list is managed by The MITRE Corporation<sup>1</sup>. The CPE is the dictionary of all software product and applications, operating systems and hardware devices which provides identification and naming for each, the official CPE dictionary can be obtained from NVD repository<sup>2</sup> and provided in XML format. The CVSS is a scoring system for the software flaw vulnerabilities, and The CCE is a dictionary of systems configuration and settings issues [4].

The CVE list is not a vulnerabilities data repository<sup>3</sup> is just names/IDs list, and NVD is one of vulnerabilities databases based on the CVE list and it provides a data feed for SCAP content such as the XML vulnerability feed which contains the cyber security software issues and it provides CVE link and a CVSS base score and CPE mapping for each vulnerability record [3].

<sup>1</sup> <https://www.mitre.org/>

<sup>2</sup> <https://nvd.nist.gov/cpe.cfm>

<sup>3</sup> The list of vulnerabilities databases list can be found at [https://cve.mitre.org/compatible/product\\_type.htmlDatabase#Vulnerability](https://cve.mitre.org/compatible/product_type.htmlDatabase#Vulnerability)

## 4 Alternatives to NVD Repository





## 6 Conclusion

The results in this section are a refined version

## References

1. <https://scap.nist.gov/>
2. <https://www.nist.gov/>
3. <https://nvd.nist.gov/>
4. The Technical Specification for the Security Content Automation Protocol(SCAP) NIST Special Publication 800-126 Revision 3