

SCAP

<https://youtu.be/JBc6542DL-4>

시스템 보안관리 업무 자동화

- 보안관리 대상이 되는 시스템의 복잡성

시스템마다 어떤 보안 설정이 필요한지 판단하는데 어려움
검증하는 관리에 있어서도 어려움이 발생

- 새로운 위협에 대한 빠른 대응 요구

일반적으로 새롭게 발견되는 취약점의 개수가 매우 많음
중요도가 높은 취약점을 판단하여 우선순위를 설정, 제거

- 상호운용성

시스템 보안 도구들이 각기 자신들만의 방법 및 콘텐츠를 사용
사용자에게 혼란

SCAP(Security Content Automation Protocol)



현재 패치 상태 확인



시스템 보안설정 모니터링

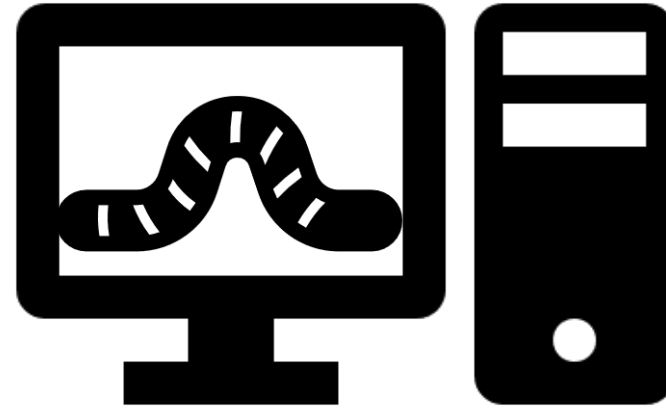


시스템 침해 징후 검사

시스템 보안관리 업무를 수행하는데 있어서 **자동화 및 표준화된 방법을** 제공하려는 목적

소프트웨어의 설정 및 취약점을 표준화된 방법으로 연관시키기 위한 프레임워크

SCAP(Security Content Automation Protocol)



SCAP는 조직이 따를 수 있는 허용 된 보안 표준을 제공

미리 결정된 보안 기준에 따라 컴퓨터, 소프트웨어 및 기타 장치를 검색

조직의 보안 유지에 대한 혼란 방지

SCAP 릴리즈

NIST에서 규격 개발 주도

SCAP 버전 1.0 (2009 년 11 월)

SCAP 버전 1.1 (2011 년 2 월)

SCAP 버전 1.2 (2011 년 9 월)

SCAP 버전 1.3 (2018 년 2 월)

SCAP 버전 2

네트워크 장비, 사물 인터넷 (IoT) 및 모바일 장치 포함

엔드 포인트 유형을 확장

SCAP 구성

- 프로토콜

소프트웨어 결함 과 설정 정보를 교환하기 위해서 필요한 포맷 및 명명 법 등의 표준화
기존 표준규격 등을 인용하여 사용

- 콘텐츠

SCAP에서 처리하는 소프트웨어 결함 및 보안설정 정보
국가취약점DB(NVD)는 CPE와 CVE 정보를 제공
MITRE에서 CCE 정보와 OVAL DB 제공

SCAP 구성

Enumerations

- CCE™: Common Configuration Enumeration
- CPE™: Common Platform Enumeration
- CVE®: Common Vulnerabilities and Exposures Metrics
- CVSS: Common Vulnerability Scoring System
- CCSS: Common Configuration Scoring System

Languages

- XCCDF: The Extensible Configuration Checklist Description Format
- OVAL®: Open Vulnerability and Assessment Language

:

NVD(National Vulnerabilites Database)

- 미국 정부는 대응책이 마련된 취약점에 대하여 공유 필요성 느낌
- 1999년 미 정부 산업표준 기관인 NIST에 의해 NVD를 구축하여 운영

CVE

단일 취약점 식별자 체계
한가지 취약점에 대해 서로 다른
취약점 데이터 베이스들이
상이한 분석 방지

CWE

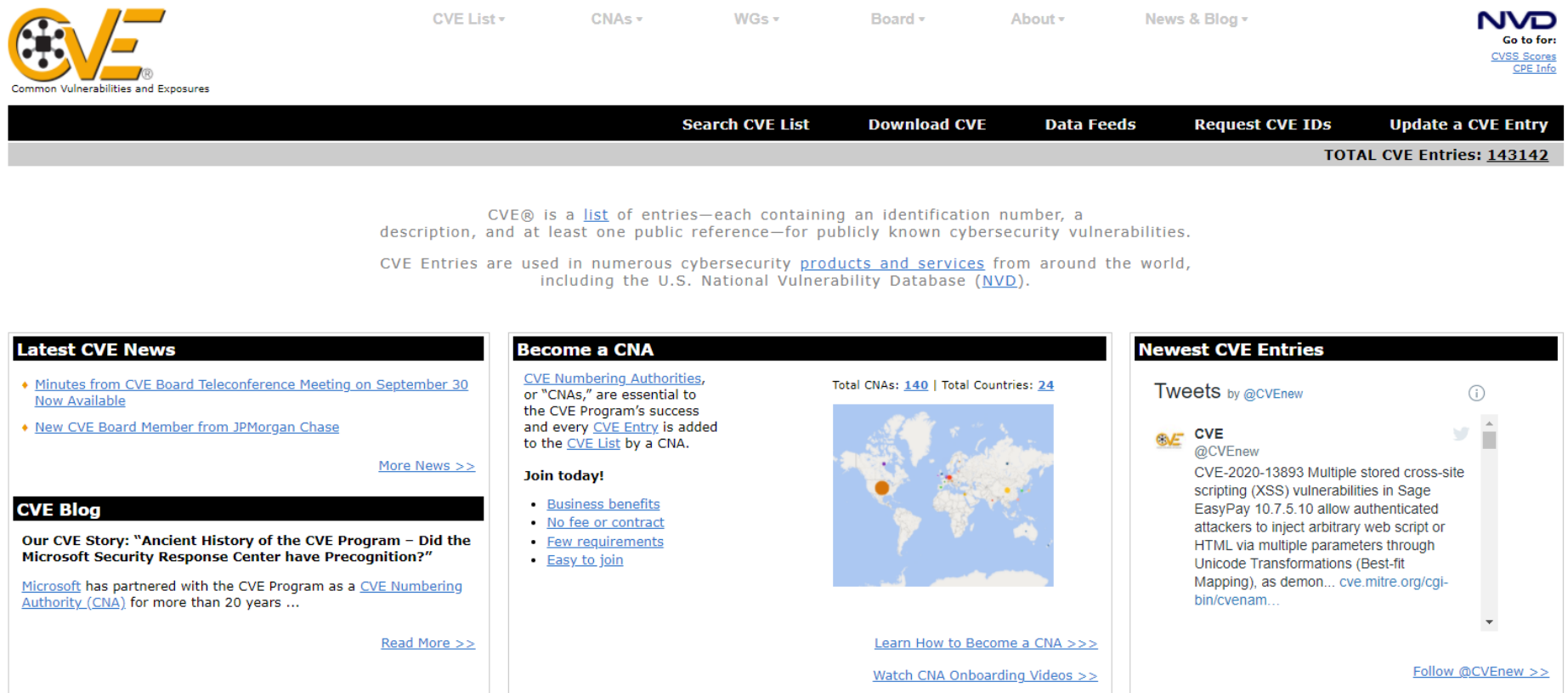
하드웨어, 운영체제, 응용프로그램
및 플랫폼을 식별하기 위한
목록

OVAL

NVD 정보를 활용하기위해 컴퓨터
시스템 보안설정 상태 검사 언어

CVE(Common Vulnerabilities and Exposures)

CVE를 통해 취약점에 “CVE-XXXX-XXXX”와 같은 고유의 식별 번호 부여
동일 취약점에 대한 서로 다른 정보들을 동일 취약점 정보로 판단하도록 도움



The screenshot shows the CVE website homepage. At the top is the CVE logo (Common Vulnerabilities and Exposures) and a navigation bar with links: CVE List, CNAs, WGs, Board, About, and News & Blog. On the right is the NVD logo with links to CVSS Scores and CPE Info. Below the navigation bar is a search bar and a table with links: Search CVE List, Download CVE, Data Feeds, Request CVE IDs, and Update a CVE Entry. A banner below the table states "TOTAL CVE Entries: 143142". The main content area explains that CVE is a list of entries with identification numbers, descriptions, and public references. It mentions that CVE Entries are used in numerous cybersecurity products and services, including the U.S. National Vulnerability Database (NVD). Below this are three sections: "Latest CVE News" with links to minutes from a board meeting and a new board member; "Become a CNA" with a list of benefits and a world map showing CNA locations; and "Newest CVE Entries" with a tweet about CVE-2020-13893.

Latest CVE News

- [Minutes from CVE Board Teleconference Meeting on September 30 Now Available](#)
- [New CVE Board Member from JPMorgan Chase](#)

[More News >>](#)

CVE Blog

Our CVE Story: "Ancient History of the CVE Program – Did the Microsoft Security Response Center have Precognition?"

[Microsoft](#) has partnered with the CVE Program as a [CVE Numbering Authority \(CNA\)](#) for more than 20 years ...

[Read More >>](#)


Become a CNA

[CVE Numbering Authorities](#), or "CNAs," are essential to the CVE Program's success and every [CVE Entry](#) is added to the [CVE List](#) by a CNA.

Join today!

- [Business benefits](#)
- [No fee or contract](#)
- [Few requirements](#)
- [Easy to join](#)

Total CNAs: **140** | Total Countries: **24**



[Learn How to Become a CNA >>>](#)

[Watch CNA Onboarding Videos >>](#)

Newest CVE Entries

Tweets by @CVEnew

CVE
@CVEnew

CVE-2020-13893 Multiple stored cross-site scripting (XSS) vulnerabilities in Sage EasyPay 10.7.5.10 allow authenticated attackers to inject arbitrary web script or HTML via multiple parameters through Unicode Transformations (Best-fit Mapping), as demon... [cve.mitre.org/cgi-bin/cvenam...](#)

[Follow @CVEnew >>](#)

CVE 제공 정보 및 항목

[Printer-Friendly View](#)

CVE-ID

CVE-1999-0067

[Learn more at National Vulnerability Database \(NVD\)](#)

• [CVSS Severity Rating](#) • [Fix Information](#) • [Vulnerable Software Versions](#) • [SCAP Mappings](#) • [CPE Information](#)

Description

phf CGI program allows remote command execution through shell metacharacters.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- [AUSCERT:AA-96.01](#)
- [BID:629](#)
- [URL:http://www.securityfocus.com/bid/629](http://www.securityfocus.com/bid/629)
- [BUGTRAQ:19960923 PHF Attacks - Fun and games for the whole family](#)
- [CERT:CA-1996-06](#)
- [URL:http://www.cert.org/advisories/CA-1996-06.html](http://www.cert.org/advisories/CA-1996-06.html)
- [OSVDB:136](#)
- [URL:http://www.osvdb.org/136](http://www.osvdb.org/136)
- [XF:http-cgi-phf](#)

Date Entry Created

19990929

Disclaimer: The [entry creation date](#) may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

This is an entry on the [CVE List](#), which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS:

You can also search by reference using the [CVE Reference Maps](#).

For More Information: [CVE Request Web Form](#) (select "Other" from dropdown)

[BACK TO TOP](#)



CWE(Common Weakness Enumeration)

- NVD, OWASP, JVN iPedia, 보안 업체 등에서 업계 공통의 기준으로 사용되는 취약점 유형 목록
- SQL 인젝션, 크로스 사이트 스크립팅, 버퍼 오버플로 등의 다양한 소프트웨어의 취약점을 식별하기 위해 취약점 유형을 체계적으로 목록화 하여 제공

CWE 구조

- CWE-ID와 같은 식별자를 부여하여 계층구조로 체계화
- View, Category, Weakness, Compound Element

View

취약점 유형을 선택 하여 모아놓은 것

CWE-699 : 개발자관점
CWE-1000 : 연구자 관점

CWE-658 : C언어
CWE-660 : JAVA

Weakness

클래스(추상적)
경쟁조건 취약점

베이스(의존성 X)
공유데이터에 대한
비동기엑세스

변형(기술, 자원 문맥 식별)
다른 세션에서 해당 세션 식별에 따른 유출

Category

공통적인 특성의 취약점

CWE-310 : 암호화 문제 취약점
CWE-355 : 사용자 인터페이스 관련

Compound Element

여러 요인으로 인한 취약점

정수 오버플로우로 인한 버퍼 오버플로우

Oval(Open Vulnerability and Assessment Language)

- 컴퓨터 시스템의 보안 설정 상태를 검사하기 위한 언어 보안 검사 방법을 정의한 데이터
- OVAL 인터프리터
정의 데이터에 명시된 검사 방법에 따라 보안 설정을 테스트

Oval 구조

- XML 기반으로 보안 프로그래밍 방식

```
▼<tests>
▼<rpminfo_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" check="at least one" comment="kernel is earlier than 0:2.6.18-128.4.1.el5" id="oval:com.redhat.rhsa:tst:20091193001" version="673">
  <object object_ref="oval:com.redhat.rhsa:obj:20091193001"/>
  <state state_ref="oval:com.redhat.rhsa:ste:20091193001"/>
</rpminfo_test>
▼<rpminfo_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" check="at least one" comment="kernel is signed with Red Hat redhatrelease key" id="oval:com.redhat.rhsa:tst:20091193002"
version="673">
  <object object_ref="oval:com.redhat.rhsa:obj:20091193001"/>
  <state state_ref="oval:com.redhat.rhsa:ste:20091193002"/>
</rpminfo_test>
...

▼<objects>
▼<rpminfo_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" id="oval:com.redhat.rhsa:obj:20091193001" version="673">
  <name>kernel</name>
</rpminfo_object>
▼<rpminfo_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" id="oval:com.redhat.rhsa:obj:20091193002" version="673">
  <name>kernel-PAE</name>
</rpminfo_object>
▼<rpminfo_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" id="oval:com.redhat.rhsa:obj:20091193003" version="673">
...

▼<states>
▼<rpminfo_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" id="oval:com.redhat.rhsa:ste:20091193001" version="673">
  <arch datatype="string" operation="pattern match">i686|ia64|ppc64|s390x|x86_64</arch>
  <evr datatype="evr_string" operation="less than">0:2.6.18-128.4.1.el5</evr>
</rpminfo_state>
▼<rpminfo_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" id="oval:com.redhat.rhsa:ste:20091193002" version="673">
  <signature_keyid operation="equals">5326810137017186</signature_keyid>
</rpminfo_state>
▼<rpminfo_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" id="oval:com.redhat.rhsa:ste:20091193003" version="673">
```

CPE(Common Playform Enumeration)

- 공용 플랫폼 목록
- 하드웨어, 운영 체제, 응용프로그램과 같은 플랫폼을 식별하는 구조화된 명칭 체계를 규정
- 부여한 명칭은 CPE 사전으로 규정되어 2008년 NIST에 의해 출판
- 일정한 기준을 갖고 취약점 검색 또는 분류 할 수 있다는 장점
- CPE 구조
cpe : / (타입)(업체 이름): (제품명) (버전)(업데이트버전)(언어)

XCCDF, ARF

XCCDF(Extensible Configuration Checklist Description Format)

보안 체크리스트, 벤치 마크 및 관련 문서를 작성하기위한 사양 언어

ARF (Asset Reporting Format)

자산에 대한 정보의 전송 형식과 자산과 보고서 간의 관계를 표현하는 데이터 모델



SCAP 사용 절차

1. CCE, CVE, CPE 등을 이용해서 정보시스템의 취약점과 보안설정을 생산하고 이를 XCCDF로 기술
2. 앞서 생산한 보안설정에 따라 점검항목을 생산하여 OVAL로 기술한다.
3. 점검대상 시스템에서 보안설정 정보를 수집
4. 점검항목과 실제 수집된 정보를 비교
5. 점검결과에 따라 보고서를 ARF에 따라 작성

OpenSCAP

- XCCDF (Extensible Configuration Checklist Description Format)를 활용하는 감사 도구입니다.
- CPE, CCE 및 OVAL과 같은 다른 사양과 결합하여 SCAP 검증 제품에서 처리할 수 있는 SCAP 표현 체크리스트를 생성

취약성 스캔 수행

• Red Hat Enterprise Linux 6.7

1. Openscap 설치

```
# yum install openscap-scanner
```

2. 보안정책 OVAL 설치

```
$ wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml
```

3. 스캔 실행

```
$ oscap oval eval --results rhsa-results-oval.xml --report oval-report.html Red_Hat_Enterprise_Linux_6.xml
```

4. 출력

```
$ oscap oval generate report results-oval.xml > report.html
```

OVAL Definition Results				
ID	Result	Class	Reference ID	Title
oval:com.redhat.rhsa:def:20151852	false	patch	[RHSA-2015-1852-00], [CVE-2015-4500], [CVE-2015-4509], [CVE-2015-4517], [CVE-2015-4519], [CVE-2015-4520], [CVE-2015-4521], [CVE-2015-4522], [CVE-2015-7174], [CVE-2015-7175], [CVE-2015-7176], [CVE-2015-7177], [CVE-2015-7180]	RHSA-2015:1852: thunderbird security update (Important)
oval:com.redhat.rhsa:def:20151841	false	patch	[RHSA-2015-1841-00], [CVE-2015-1303], [CVE-2015-1304]	RHSA-2015:1841: chromium-browser security update (Important)
oval:com.redhat.rhsa:def:20151840	false	patch	[RHSA-2015-1840-00], [CVE-2015-6906]	RHSA-2015:1840: openldap security update (Important)
oval:com.redhat.rhsa:def:20151834	false	patch	[RHSA-2015-1834-02], [CVE-2015-4500], [CVE-2015-4506], [CVE-2015-4509], [CVE-2015-4511], [CVE-2015-4517], [CVE-2015-4519], [CVE-2015-4520], [CVE-2015-4521], [CVE-2015-4522], [CVE-2015-7174], [CVE-2015-7175], [CVE-2015-7176], [CVE-2015-7177], [CVE-2015-7180]	RHSA-2015:1834: firefox security update (Critical)
oval:com.redhat.rhsa:def:20151833	false	patch	[RHSA-2015-1833-00], [CVE-2015-5165]	RHSA-2015:1833: qemu-kvm security update (Moderate)
oval:com.redhat.rhsa:def:20151814	false	patch	[RHSA-2015-1814-00], [CVE-2015-5567], [CVE-2015-5568], [CVE-2015-5570], [CVE-2015-5571], [CVE-2015-5572], [CVE-2015-5573], [CVE-2015-5574], [CVE-2015-5575], [CVE-2015-5576], [CVE-2015-5577], [CVE-2015-5578], [CVE-2015-5579], [CVE-2015-5580], [CVE-2015-5581], [CVE-2015-5582], [CVE-2015-5584], [CVE-2015-5587], [CVE-2015-5588], [CVE-2015-5589], [CVE-2015-6676], [CVE-2015-6677], [CVE-2015-6678], [CVE-2015-6679], [CVE-2015-6682]	RHSA-2015:1814: flash-plugin security update (Critical)
oval:com.redhat.rhsa:def:20151741	false	patch	[RHSA-2015-1741-00], [CVE-2015-3281]	RHSA-2015:1741: haproxy security update (Important)
oval:com.redhat.rhsa:def:20151715	false	patch	[RHSA-2015-1715-00], [CVE-2015-3247]	RHSA-2015:1715: spice-server security update (Important)
oval:com.redhat.rhsa:def:20151712	false	patch	[RHSA-2015-1712-00], [CVE-2015-1291], [CVE-2015-1292], [CVE-2015-1293], [CVE-2015-1294], [CVE-2015-1295], [CVE-2015-1296], [CVE-2015-1297], [CVE-2015-1298], [CVE-2015-1299]	RHSA-2015:1712: chromium-browser



Q & A

