CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

OVAL

CCERT-PUBDOC-2009-01-251

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

OVAL (eng. Open Vulnerability and Assessment Language) standard omogućava procjenu ranjivosti sustava ili nepravilnosti u konfiguraciji. Razvijen je od strane MITRE (http://www.mitre.org/) organizacije (u suradnji s OVAL zajednicom), a financiran od strane US-CERT (http://www.us-cert.gov/) organizacije.

Sastoji se od OVAL jezika i OVAL repozitorija, a dodatno je razvijen i OVAL prevodilac. OVAL jezik definira tri sheme koje se koriste prilikom ocjenjivanja sustava te djeluje na mnogim područjima (npr. izdavanje sigurnosnih preporuka, upravljanje dodacima i sl.). OVAL repozitorij daje pregled postojećih OVAL definicija, entiteta koji sadrže jedan ili više testova te omogućuju njihovo izvođenje. Prevodilac je razvijen kako bi se korisnicima omogućilo prezentiranje raznih prednosti testiranja.

Standard rastavlja proces procjene ranjivosti u tri faze:

- Prikupljanje informacija o ranjivostima i konfiguraciji,
- Analiziranje sustava,
- Pružanje izvješća.

OVAL standard rezultat je suradnje OVAL zajednice, OVAL Board organizacije i OVAL moderatora. Svaki korisnik koji je na neki način uključen u sigurnost računarskih sustava može se uključiti i u razvoj ovog standarda, raspravljati o ranjivostima, definicijama ili pridonijeti na neki drugi način.

Ovaj dokument daje opis OVAL standarda, jezika, repozitorija i prevodioca. Također su dane informacije o trenutnom stanju OVAL standarda, načinu uporabe te načinu doprinosa. Na kraju dokumenta nalaze se i pregled predviđanja razvijanja ovog standarda.

2. OVAL standard

OVAL (eng. Open Vulnerability and Assessment Language) je nacionalni standard o informacijskoj sigurnosti. Cilj mu je promocija otvorenog i javno dostupnog sadržaja o sigurnosti te standardiziranje prijenosa takvih informacija širokim spektrom sigurnosnih alata i usluga.

Standard uključuje:

- **OVAL jezik** – namijenjen kodiranju detalja sustava,
- **OVAL repozitorij** – skup sadržaja.

Zajednica pruža razne dokumente o OVAL standardu, jeziku i repozitoriju koje je moguće pronaći na web stranici:

http://oval.mitre.org/oval/about/documents.html.

U nastavku dokumenta dan je prikaz povijesti razvoja OVAL standarda i njegova svrha, te su navedene skupine korisnika kojima je sam standard namijenjen.

2.1. Kratka povijest razvoja

Prve inačice OVAL definicija, shema, prevodioca i ostalih podataka imale su SQL oblik, a razvijene su 2005.g. Postojala je samo shema definicija, a bila je dostupna za Microsoft Windows, Sun Solaris, Red Hat Linux, Debian Linux, i Hewlett Packard-Unix platforme. Razvoj navedenih inačica prekinut je 2005.g. te ne postoji odgovarajuća nadogradnja. Ipak moguće ih je preuzeti preko navedene poveznice:

http://oval.mitre.org/oval/archive/sql/index.html

Slijedeće inačice napuštaju SQL format te prelaze na korištenje XML jezika. Također, razvijene su tri sheme: definicija, karakteristika sustava i rezultata te je takav oblik zadržan sve do danas. Prva inačica razvijana u opisanom obliku je inačica 3, i službeno je objavljena 31. ožujka 2005.

Iste godine razvijana je nova inačica 4.0, koju su slijedile dvije inačice s nekim malim izmjenama (4.1 i 4.2).

16. lipnja 2006.g. službeno je objavljena inačica 5.0 koja je uvela razne promjene. Nakon nje izdano je 5 inačica s manjim izmjenama (5.1, 5.2, 5.3, 5.4 i 5.5).

Popis svih inačica, zajedno s poveznicama preko kojih je moguće preuzeti sve ranije inačice nalazi se na web stranici:

http://oval.mitre.org/oval/archive/index.html

Opis trenutne inačice OVAL standarda (5.5) dostupan je u odjeljku „Razvoj OVAL standarda“, a očekivani razvoj u budućnosti u dijelu „Očekivanja u budućnosti“.

2.2. Svrha standarda

Do razvoja OVAL standarda nije postojala osnova za administriranje sustava ili za omogućavanje otkrivanja ranjivosti programa i konfiguracijskih problema krajnjim korisnicima. Mnoge informacije bile su dostupne u tekstualnom obliku iz izvora koji analiziraju ranjivosti kao što su davatelji usluga, razne agencije vlade, prodavači alata i tvrtke koje se bave sigurnošću računala. Ali takva dostupnost informacija zahtijevala je od administratora mnogo vremena i rada kako bi otkrili određenu ranjivost ili konfiguracijski problem na lokalnom sustavu.

OVAL standard (još) nije alat za provjeru ranjivosti, nego jezik koji pomaže otkriti probleme koji postoje na sustavu. Dopušta dijeljenje tehničkih detalja o postojanju ili odsutnosti ranjivosti na računarskim sustavima. Također postoji mogućnost osobnog pregleda pojedine definicije kako bi se dobio uvid u

način otkrivanja ranjivosti. Opisani scenarij čini potpunu suprotnost zatvorenim metodama provjere ranjivosti koje su obično u privatnom vlasništvu.

Baze o sigurnosnim nedostacima sadrže neke informacije koje OVAL standard ne sadrži, kao npr. ozbiljnost problema, način zlouporabe (lokalno/udaljeno) i sl. Umjesto toga, OVAL definicije pružaju detaljne metode za provjeru konfiguracijskih parametara kako bi se otkrilo postojanje pogrešaka ili potvrdila njihova odsutnost. Baze podataka o sigurnosti jako rijetko sadrže ovakve tehničke detalje.

Javna dostupnost OVAL definicija promovira standardiziranje procjene ranjivosti i konfiguracije te pruža dosljedan skup informacija koje je moguće reproducirati. Alati za skupljanje konfiguracijskih parametara mogu biti kombinirani sa OVAL sadržajem kako bi omogućili standardiziranje procjene što dovodi do točnog otkrivanja pogrešaka.

U svrhu zaštite, OVAL je moguće koristiti samo u obliku mjera sprječavanja napada. Nakon uporabe OVAL definicija ili OVAL sigurnosnih proizvoda/usluga kako bi se otkrio problem na sustavu, korisnik može iskoristiti dobivene informacije za stvaranje novih programskih rješenja. Ipak, OVAL ne podržava ispravak problema pa korisnik mora sam otkriti način za to, potražiti nadogradnju ili odgovarajuće upute od pružatelja određenih usluga ili alata.

2.3. Namjena standarda

OVAL standard namijenjen je:

- istraživačima sigurnosti – pronalaženje sigurnosnih problema te konfiguracijskih nedostataka,
- prodavačima programskih rješenja – otkrivanje nedostataka programa prije puštanja u prodaju, kao i održavanje alata tokom razvoja i prodaje,
- administratorima sustava – pronalaženje sigurnosnih rupa na sustavima u svrhu njihova uklanjanja,
- krajnjim korisnicima – ispitivanje proizvoda te otkrivanje nedostataka kako bi potražili odgovarajuću nadogradnju ili informacije o rješavanju problema.

Za prodavače operacijskih sustava i programa, definiranje standardnog načina otkrivanja ranjivosti uklanja potrebu za korištenjem koda kao alata za procjenu. Upravo takve standardizirane načine detektiranja nedostataka moguće je pronaći u OVAL standardu. Dodatnu poteškoću donose zatvoreni testovi za provjeru ranjivosti, koje prodavači alata implementiraju u jeziku nerazumljivom široj javnosti (a najčešće ni sam programski kod nije dostupan javnosti). OVAL standard definira jezik jednostavan za korištenje te jedinstven za sve alate.

3. OVAL jezik

OVAL jezik omogućuje sukladnost između sigurnosnih alata podržavajući standardni XML jezik kojim izmjenjuju informacije. Omogućuju raznim alatima izvođenje određenih zadataka. Na primjer, alat za procjenu ranjivosti može utjecati na usluge istraživanja ranjivosti ili automat za provjeru odstupanja može utjecati na vladino upravljanje sigurnošću.

OVAL jezik uvodi tri glavna koraka prilikom procjene procesa:

1. **predstavljanje informacija** o konfiguraciji sustava koji se testira,
2. **analiziranje sustava** radi ispitivanja postojanja posebnih stanja (ranjivosti, nepravilnosti u konfiguraciji i sl.) i
3. **pružanje izvješća** o rezultatima.

3.1. Osnovne značajke

Podjelom OVAL jezika u tri zasebne sheme koje predstavljaju tri faze provjere procesa omogućeno je organiziranje implementacije samo onih dijelova OVAL jezika koji su doista potrebni pojedinim alatima. Prednost ovoga je dostupnost OVAL jezika širem rasponu sigurnosnih alata, što omogućuje veću kompatibilnost.

U nastavku su navedena neka područja rada OVAL jezika.

3.1.1. Izdavanje sigurnosnih preporuka

Potreba prodavača aplikacija i operacijskih sustava je objava informacija o ranjivosti u standardnom obliku.

Dobit takve organizacije podataka za korisnike je u slijedećem:

- Pružanje alata s izravnim pristupom sadržaju koji može biti iskorišten za pristup važnim dijelovima sustava,
- Pomicanje upravljanja tehničkim detaljima ranjivosti od osobe koja razvija alat za skeniranje do osobe koja razvija ranjivi program.

3.1.2. Procjena ranjivosti

Trenutno organizacije koje razvijaju alate za procjenu ranjivosti također trebaju zaposliti tim za razvoj sadržaja. Uloga ovog tima je istražiti ranjivosti kada postanu poznate, prikupiti sve dostupne informacije za danu ranjivost, provesti razne testove za otkrivanje ranjivosti, razviti testove u jeziku istim kao i alat te se pritom pridržavati svih propisa.

Za prodavače, posjedovanje informacija o ranjivostima organiziranim u standardnom obliku dopušta im da brzo iskoriste podatke iz raznih izvora i povećaju funkcionalnost alata.

Iz perspektive korisnika alata, osnovni zahtjev za posjedovanjem sadržaja standardnog oblika je olakšavanje procesa procjene ranjivosti te pružanje mogućnosti usporedbe alata. Dostupnost dobro dokumentiranog, standardnog oblika pruža korisnicima potrebne informacije kako bi razumjeli detalje problema i ocijenili korist od uporabe određenog alata. Otvorenost standarda također pruža korisnicima priliku da generiraju vlastite navode i prevode ih. Prilikom provedbe usporedbe alata, preko posebne grupe definicija, svaki testirani alat treba dati iste rezultate. Ako to nije slučaj, korisniku se ostavlja da odredi koji su rezultati najpouzdaniji. Krajnji rezultat je da se korisnici mogu fokusirati na odabir alata sa značajkama koje najbolje odgovaraju njihovim potrebama, a manje na složenije probleme ispravnog otkrivanja ranjivosti.

3.1.3. Upravljanje dodacima

Potrebe upravljanja dodacima slične su potrebama procjene ranjivosti. Postojanje prikupljenih podataka u standardnom obliku omogućuje generiranje sadržaja potrebnog za izgradnju dodataka na brži i jednostavniji način. Također zahtjeva se jednostavnost korištenja rezultata procjene ranjivosti od raznih sustava za provjeru ranjivosti. Kada bi se rezultati pružali u standardnom obliku, međudjelovanje i usporedba alata ne bi bila kompleksna.

3.1.4. Upravljanje konfiguracijom

Alati za upravljanje konfiguracijom uspoređuju trenutna konfiguracijska stanja s ispravnim ili zadanim stanjem te daju izvještaj s rezultatima. Postoje brojni javno dostupni vodiči o ispravnoj konfiguraciji, a neke je moguće pronaći na web stranici NSA vodiča (National Security Agency Configuration Guides):

http://www.nsa.gov/snac/.

U mnogim slučajevima ovi vodiči postoje samo u pisanom obliku, a IT osoblje ima zadatak dovesti ga u oblik pogodan za primjenu. Postoje i automatizirana rješenja, ponajprije alati Centra za Mjerenje Performansi Internet Sigurnosti (eng. Center for Internet Security's Benchmark), koji mogu ispitivati sustav tražeći razlike između konfiguracije i pouzdano ispitanih ispravnih rješenja. Na žalost, ovi alati često ovise o određenom obliku podataka, što otežava uvođenje novih politika alatima ili prijenos podataka do drugog alata.

Postojanje standardnog jezika za zadavanje konfiguracije sustava donosi mnoge pogodnosti ovom području. Kao prvo, svaku postavku konfiguracije potrebno je napisati samo jednom, a može ju koristiti bilo koji alat. Zatim, organizacije mogu lakše razviti i upravljati svojim standardima konfiguracije, jer to zahtjeva samo učenje jednog jezika za sve alate, a ne više jezika specifičnih za više alata. Na kraju, oslobađanje ovisnosti jezika od alata omogućuje prodavačima alata usmjeravanje pozornosti na značajke alata i funkcionalnost.

3.1.5. Revizije i provjere revizija

Provjera revizija je odgovorna za pružanje izvješća o stanju u danom vremenu u prošlosti. Postoje dva osnovna zahtjeva u ovom području:

- Prikupljanje konfiguracijskih informacija na razini koja omogućuje organizacijama upravljanje, praćenje i rekonstruiranje prijelaza stanja iz jednog u drugo i
- Pohranjivanje podataka u standardnom obliku, što osigurava neovisnost o posebnom alatu (koji može, ali i ne mora biti dostupan u određenom vremenu izrade revizija).

3.1.6. SIMS

SIMS (eng. Security Information Management Systems) ovisi o izlaznom obliku mnogih sigurnosnih alata te alata za upravljanje revizijama i konfiguracijom, kao i njihovih sredstava. Općenito, ako SIMS zahtjeva jednostavniji oblik podataka, on je više fleksibilan i potencijalan alat. Zajedno s upravljanjem dodacima, standardizira izmjenu podataka među raznim alatima što pojednostavljuje potrebe pri suradnji te pruža krajnjim korisnicima široko područje izbora aplikacija.

3.1.7. Zalihe sustava

Osnovni problem (ne samo kod sigurnosnih alata, nego bilo kojeg alata koji izvodi neki oblik ocjene stanja računala) je određivanje atributa promatranog sustava (npr. operacijski sustav, razina dodataka, instalirane aplikacije i sl.). Trenutno, ne postoji globalno prihvaćena metoda za to, kao ni osnovni način predstavljanja prikupljenih podataka kako bi ih drugi alati mogli koristiti. Ipak potreba za ovom mogućnošću je dobro poznata i njena uporaba bi bila široko raširena.

3.2. Sheme

OVAL zajednica je razvila tri sheme pisane u XML (eng. Extensible Markup Language) jeziku kako bi poslužili kao okružje i rječnik za OVAL jezik. Te tri sheme odgovaraju trima koracima u procesu procjene:

1. **shema karakteristika sustava** (eng. OVAL System Characteristics schema),
2. **shema definicija** za izražavanje posebnih stanja (eng. OVAL Definition schema),
3. **shema za rezultate** (eng. OVAL Results schema).

3.2.1. Način rada

Način komunikacije tri navedene sheme opisan je u nastavku dokumenta:

1. Prikupljanje informacija

OVAL shema o karakteristikama sustava definira XML format za predstavljanje informacija o konfiguraciji sustava, koji sadrži parametre operacijskih sustava, postavke raznih aplikacija i druge varijable vezane uz sigurnost. Shema pruža „bazu podataka" karakteristika sustava preko kojih OVAL definicije mogu biti korištene za analiziranje postojanja neregularnih stanja. Shema također može koristiti neki od oblika razmjene informacija kako bi se ostvarila suradnja s nekim od pogodnih alata. Prilikom korištenja datoteke ove sheme, druge aplikacije ne moraju izvoditi prikupljanje podataka, nego iskoristiti prikupljane podatke kako bi obavili analizu.

2. Standardiziranje testova

Shema OVAL definicija je okružje za pisanje OVAL definicija u XML jeziku. OVAL definicije definiraju detalje specifičnih stanja (ranjivosti, neotpornosti i sl.) omogućavajući automatizirano testiranje sustava. Također, pruža raspravu o detaljima otkrivanja problema bilo da se radi o ranjivosti na sustavu, pogrešci u konfiguraciji ili nepravilnostima u dodacima.

Postoje dva dijela sheme za pisanje OVAL definicija:

- Jezgrena shema – namijenjena opisu osnovnih formata.
- Shema individualnih komponenata – namijenjena testovima koji su karakteristični za određenu OS platformu ili aplikaciju. Na primjer, UMIX shema sadrži testove za UNIX platformu, a Windows shema za Windows.

3. Rezultati provjere ranjivosti

Shema rezultata testa definira standardni XML oblik za izvještaj o rezultatima ispitivanja sustava. Krajnji podaci izražavaju trenutno stanje usporedbe konfiguracije sustava i skupine OVAL definicija. Spomenuta shema omogućuje aplikacijama da koriste podatke, interpretiraju ih i poduzmu potrebne akcije kako bi se smanjile ranjivosti i konflikti u konfiguraciji. Na primjer, instaliranje dodataka, ažuriranje postavka konfiguracije sustava i/ili poduzimanje mjera kako bi se spriječio pristup zaraženom sustavu.

Jedan od alata koji pruža odgovarajući oblik rezultata drugim alatima za analizu je OVAL prevodilac.

Neki od poznatijih besplatnih alata koji koriste OVAL su:

- NetIQ Secure Configuration Manager 5.6

  http://www.netiq.com/products/configurationmgmt/default.asp

- C5 Compliance Platform Version 3.0

  http://www.secure-elements.com/products/

Popis ostalih alata dostupan je na slijedećoj poveznici:

http://oval.mitre.org/compatible/index.html.

4. OVAL repozitorij

OVAL repozitorij je središnje mjesto OVAL zajednice za raspravu, analiziranje i pohranu OVAL definicija. Ostali repozitoriji zajednice također pohranjuju OVAL sadržaj, što može uključiti OVAL polja sa karakteristikama sustava i OVAL polja s rezultatima, ali i same definicije.

OVAL definicije su standardizirani testovi pisani u OVAL jeziku koji provjeravaju stanja računarskih sustava i otkrivaju postojanje ranjivosti programa te problema u konfiguraciji programa i/ili dodataka. OVAL definicije, koje su besplatne za uporabu i implementaciju u sigurnosne proizvode i usluge, pisane su XML jezikom te dostupne za većinu današnjih platforma.

4.1. OVAL definicije

OVAL definicije razvio je MITRE tim i članovi OVAL zajednice, što uključuje:

- OVAL Board organizaciju,
- organizacije koje sadrže proizvode i usluge koji su kompatibilni s OVAL standardom,
- članove foruma OVAL zajednice.

OVAL definicije otkrivaju prisutnost ranjivosti programa i konfiguracijskih problema bez potrebe za pregledom koda programa. Definiranjem logičkih stanja vrijednosti karakteristika sustava i atributa konfiguracije, one karakteriziraju točno koji sustav mogu imati ili imaju zadanu ranjivost. Karakteristike sustava uključuju instalirane operacijske sustave, postavke istih, instalirane aplikacije i njihove postavke . Atributi konfiguracije uključuju postavke registra, konfiguracijskih i sistemskih datoteka i sl.

Postoje 4 osnovna razreda OVAL definicija:

- **OVAL definicije o ranjivostima** (eng. OVAL Vulnerability Definitions) – Testovi otkrivaju prisutnost ranjivosti na sustavu,
- **OVAL definicije o sukladnosti** (eng. OVAL Compliance Definitions) – Testovi otkrivaju da li se postavke konfiguracije slažu sa sigurnosnom politikom,
- **OVAL definicije o zalihama** (eng. OVAL Inventory Definitions) – Testovi koji otkrivaju postavke instaliranih programa na sustavu,
- **OVAL definicije o dodacima** (eng. OVAL Patch Definitions) . Testovi otkrivaju koji su dodaci prikladni korištenoj konfiguraciji sustava.

Mješovita klasa je također dostupna za definicije koje ne pripadaj niti u jednu od četiri osnovne.

OVAL definicije o ranjivostima se temelje isključivo na CVE (eng. Common Vulnerabilities and Exposures), rječniku standardnih imena i opisa javno poznatih sigurnosnih ranjivosti, a razvijene su od strane MITRE organizacije. Više informacija o CVE moguće je pronaći na web stranici:

http://cve.mitre.org/.

Svaka definicija je označena jedinstvenim OVAL Identifikatorom (OVAL-ID), slijedećeg oblika:

"oval:Ime DNS Organizacije:ID Tip:ID Vrijednost"

Ime DNS Organizacije – ima oblik: 'org.mitre.oval',
ID Tip – označava entitet na koji se ID odnosi (def-definicija, obj-objekt, ste-stanje, tst-test ili var-varijabla),
ID Vrijednost – cjelobrojna vrijednost koji je jedinstveno povezan s DNS Imenom i ID Tipom.

Primjer:

> oval:org.mitre.oval:def:1115
> http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1115

Slika 1 prikazuje primjer OVAL definicije sa svim prethodno opisanim elementima.

Definition Id: oval:org.mitre.oval:def:1115			**Date:** 2006-10-17
Title:	IE6,SP2 PNG Image Buffer Overflow		
Description:	Buffer overflow in the PNG image rendering component of Microsoft Internet Explorer allows remote attackers to execute arbitrary code via a crafted PNG file.		
Version:	2	**Class:**	vulnerability
Status:	ACCEPTED	**Reference(s):**	CVE-2005-1211
Family:	windows		
Platform(s):	Microsoft Windows XP	**Product(s):**	Microsoft Internet Explorer
Definition Synopsis:			
• Software section o Internet Explorer 6.0 Installed XP SP2 o AND the version of mshtml.dll is less than 6.0.2900.2668 o AND NOT the patch kb883939 is installed • AND Configuration section o PNG image rendering enabled in Internet Explorer			

Slika 1. OVAL definicija

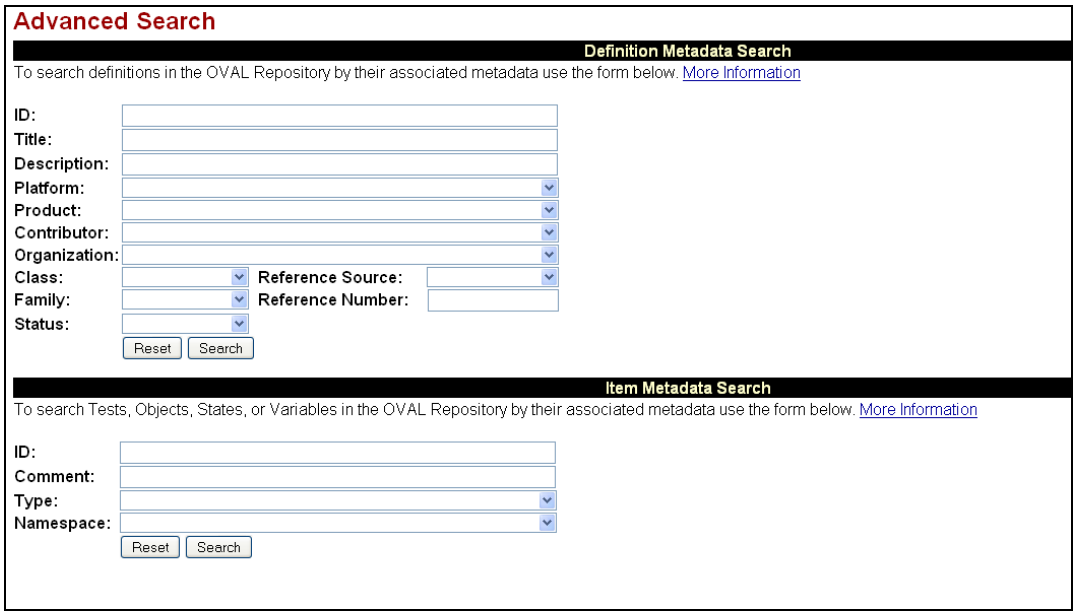
4.1.1. Podaci uključeni u OVAL definicije

Svaka OVAL definicija uključuje:

- **Meta podatke** koje se sastoje od:
  - OVAL-ID vrijednosti,
  - stanje definicije (skiciranje, privremena, prihvaćena),
  - CVE ime ili drugu reference na kojoj se temelji definicija,
  - inačicu OVAL sheme za definicije s kojom definicija radi,
  - opis sigurnosnog problema,
  - autora definicije,
  - popis suradnika koji su pomogli razvoju.
- **Sažetak** koji uključuje slijedeće:
  - Postoji ranjivost programa – što označava:
    - neki operacijski sustav,
    - ime datoteke s ranjivosti,
    - inačicu aplikacije,
    - stanje dodatka,
  - Ranjivost konfiguracije – što ukazuje:
    - da li je usluga pokrenuta,
    - posebne postavke konfiguracije,
    - rješenje.
- **Test(ove)** – može uključivati samo jedan ili više testova povezanih operatorima AND ili OR.

4.2. Pretraga repozitorija

Pretraživanje repozitorija preko OVAL-ID vrijednosti moguće je na stranicama OVAL repozitorija kako prikazuje slika 2.



Slika 2. Tražilica OVAL repozitorija

Korisnicima omogućuje pretraživanje komponenti OVAL jezika kojima je dodijeljen OVAL-ID broj što uključuje:

- OVAL definicije,
- Objekte,
- Stanja,
- Testove i
- Varijable.

Prilikom pretrage potrebno je upisati nešto od slijedećeg:

- ID definicije – pretraživanje OVAL repozitorij za jednom definicijom s posebnim ID brojem. Na primjer, pretraživanje pomoću*: oval:com.example:def:123* vraća url s traženom definicijom.
- Tip definicije i cjelobrojna vrijednost – pretraživanje OVAL repozitorija za svim definicijama s određenom cjelobrojnom vrijednosti i tipom. Na primjer, pretraživanje pomoću: *def:123* daje rezultate: oval:com.example:def:123, oval:org.mitre.oval:def:123, oval:com.abc:def:123 i sl.
- Samo cjelobrojna vrijednost – pretraživanje OVAL repozitorija za OVAL definicijama čiji ID ima zadanu cjelobrojnu vrijednost. Na primjer, zadavanjem 123 rezultat ima izgled: oval:com.example:def:123, oval:org.mitre.oval:def:123, oval:com.abc:def:123 i sl.
- ID tip i cjelobrojna vrijednost – pretraživanje OVAL repozitorija za svim definicijama koje koriste neki OVAL-ID s definiranim ID tipom i cjelobrojnom vrijednošću. Na primjer, pretraga pomoću tst:123 daje sve definicije koje koriste neki test s navedenim tipom i brojem 123.
- Koristiti ID, a ne ID definicija – pretraga za definicijama koje koriste definirani ID. Na primjer, pretraga za oval:com.example:obj:123 vraća njegov URL adresu.

Dostupno je i napredno pretraživanje preko meta podataka kombiniranjem:

- naslova,
- opisa,
- platformi,
- proizvoda,

- izdavača,
- organizacije,
- klase,
- statusa i
- izvora.

Napredna pretraga nalazi se na dolje navedenoj web stranici:

http://oval.mitre.org/repository/data/AdvancedSearch.jsp

Na sličan način moguće je pretraživati i druge entitete: testove, objekte, stanja i varijable.

4.3. OVAL prevodilac

OVAL prevodilac je besplatno dostupna implementacija koja demonstrira ocjenjivanje OVAL definicijama, a razvila ga je MITRE organizacija. Izdan je pod *BSD (eng. Berkeley Software Distribution)* licencom, i pisan u programskom jeziku C+. Temelji se na grupi definicija, a okuplja informacije o sustavu, ocjenjuje ga te generira datoteku s detaljnim rezultatima.

Demonstrira korisnost OVAL definicija i pruža ispravnu sintaksu OVAL jezika tijekom razvoja definicija. Prevodilac nije alat za skeniranje i ima jednostavno korisničko sučelje, ali njegovo pokretanje pruža popis vrijednosti rezultata za svaku ocjenjivanu definiciju.

OVAL prevodilac i svi podaci smješteni su na web stranicu SourceForge.net i dostupni preko slijedeće poveznice:

http://sourceforge.net/projects/ovaldi/

Navedena stranica uključuje:

- tražilicu ranjivosti i svojstava – pretraga ranjivosti, rješenja i novih svojstava,
- dijeljenje datoteka – za sve inačice OVAL prevodioca,
- SVN repozitorij – anonimno, moguć samo pristup čitanja,
- Wiki – osnovni izvor informacija o OVAL prevodiocu,
- forum (za pomoć) – za sva pitanja o prevodiocu.

5. Razvoj OVAL standarda

5.1. Faze razvoja

Razvoj novih inačica sadrži slijedeće faze (slika 3):

- **Pregled procesa** - Svrha pregleda procesa je potvrda da svi članovi OVAL zajednice imaju mogućnost doprinosa OVAL jeziku. Također, pruža razvijačima OVAL alata skupinu prekretnica koje im pomažu u planiranju vlastitih proizvoda da bi bili u skladu sa OVAL jezikom. Cijelim procesom upravljaju OVAL moderator, član OVAL zajednice ili organizacija koja održava OVAL i pruža važne tehničke vodiče. OVAL moderator trenutno je predstavnik MITRE korporacije.
- **Planiranje** - OVAL moderator započinje proces planiranja prikupljanjem preporuka i komentara OVAL zajednice o trenutnom OVAL jeziku. OVAL Board udruga pregleda prijedloge i određuje koji bi se trebali uključiti u novu inačicu. Trajanje ovog razdoblja je temeljeno na broju, sadržaju i važnosti promjena.
- **Skiciranje/Unutarnji pregled** - Novu inačicu OVAL jezika službeno predstavlja OVAL zajednica. Od njih se očekuje pregled sheme i prijedlog dodataka, dijelova za ukloniti te izmjena. Tijekom ovog razdoblja OVAL moderator upravlja testiranjem i izmjenama OVAL alata kako bi sve bilo u skladu sa preporukama.
- **Prva inačica** - OVAL Board ispituje da li je OVAL jezik dostigao razinu koja je dogovorena kod OVAL zajednice, a OVAL moderator provjerava ispravnost. U ovoj fazi prestaje razvoj jezika u fazi ispitivanja od strane OVAL Board organizacije. Tada prodavači alata mogu obnoviti svoje alate sa sigurnošću da će shema ostati nepromijenjena. Promjene su moguće samo ako se otkrije ozbiljni problem u predstavljenom jeziku.
- **Službeno izdavanje** - Informacija o izdavanju nove inačice OVAL jezika, uključujući OVAL definicije i OVAL prevodilac objavljuje se na web stranici OVAL zajednice. Ranije sheme i njihovi elementi arhivirani su na istoj stranici.

Slika 3. Faze razvoja OVAL standarda

5.2. Trenutna inačice OVAL jezika

1. Listopada 2008. službeno je objavljena nova inačica OVAL jezika, inačica 5.5, kao rezultat rada OVAL zajednice. Donosi manje izmjene i ne predstavlja veliki iskorak kao što je to bio slučaj kod nekih prethodnih inačica. Nova inačica potpuno je kompatibilna s prethodnom inačicom 5.4.

Dostupna je za slijedeće platforme:

- Cisco,
- FreeBSD,
- HP-UX,
- IBM AIX,
- Linux,
- Microsoft Windows.
- Sun Solaris,
- UNIX.

Popis svih izmjena, kao i njihovog stanja te preuzimanje nove inačice moguće je napraviti preko navedene poveznice:

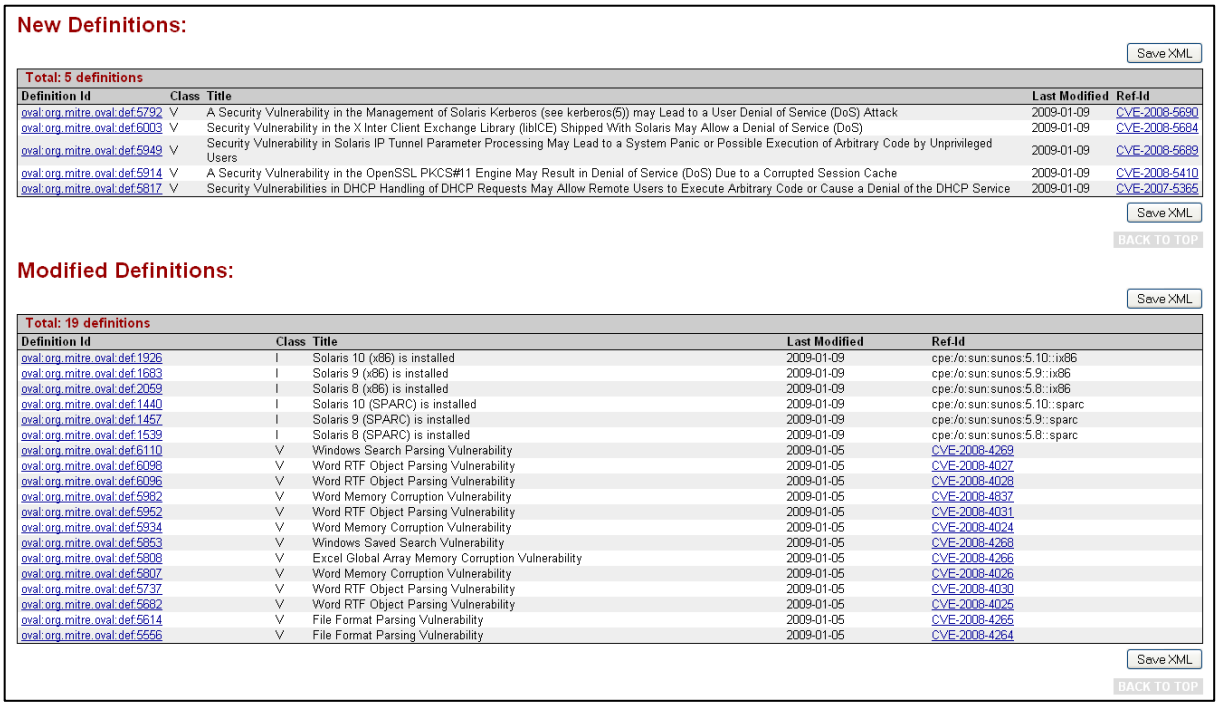
http://oval.mitre.org/language/download/schema/version5.5/index.html#new

5.3. Trenutna inačica OVAL repozitorija

OVAL definicije se svakodnevno razvijaju, na način da neki član zajednice predloži određenu izmjenu ili predloži dodavanje nove definicije. Svaku predloženu definiciju ili izmjenu prije objave provjerava tim za OVAL repozitorij. Popis izmjena objavljuje se na web stranici:

http://oval.mitre.org/repository/data/LatestUpdates

Primjer izmjena 9. siječnja 2009.g. prikazuje slika 4. Vidljivo je 5 novih definicija te izmjena 19 postojećih.



New Definitions:

Save XML

Total: 5 definitions

Definition Id	Class	Title	Last Modified	Ref-Id
oval:org.mitre.oval:def:5792	V	A Security Vulnerability in the Management of Solaris Kerberos (see kerberos(5)) may Lead to a User Denial of Service (DoS) Attack	2009-01-09	CVE-2008-5690
oval:org.mitre.oval:def:6003	V	Security Vulnerability in the X Inter Client Exchange Library (libICE) Shipped With Solaris May Allow a Denial of Service (DoS)	2009-01-09	CVE-2008-5684
oval:org.mitre.oval:def:5949	V	Security Vulnerability in Solaris IP Tunnel Parameter Processing May Lead to a System Panic or Possible Execution of Arbitrary Code by Unprivileged Users	2009-01-09	CVE-2008-5689
oval:org.mitre.oval:def:5914	V	A Security Vulnerability in the OpenSSL PKCS#11 Engine May Result in Denial of Service (DoS) Due to a Corrupted Session Cache	2009-01-09	CVE-2008-5410
oval:org.mitre.oval:def:5817	V	Security Vulnerabilities in DHCP Handling of DHCP Requests May Allow Remote Users to Execute Arbitrary Code or Cause a Denial of the DHCP Service	2009-01-09	CVE-2007-5365

Save XML

BACK TO TOP

Modified Definitions:

Save XML

Total: 19 definitions

Definition Id	Class	Title	Last Modified	Ref-Id
oval:org.mitre.oval:def:1926	I	Solaris 10 (x86) is installed	2009-01-09	cpe:/o:sun:sunos:5.10::ix86
oval:org.mitre.oval:def:1683	I	Solaris 9 (x86) is installed	2009-01-09	cpe:/o:sun:sunos:5.9::ix86
oval:org.mitre.oval:def:2059	I	Solaris 8 (x86) is installed	2009-01-09	cpe:/o:sun:sunos:5.8::ix86
oval:org.mitre.oval:def:1440	I	Solaris 10 (SPARC) is installed	2009-01-09	cpe:/o:sun:sunos:5.10::sparc
oval:org.mitre.oval:def:1457	I	Solaris 9 (SPARC) is installed	2009-01-09	cpe:/o:sun:sunos:5.9::sparc
oval:org.mitre.oval:def:1539	I	Solaris 8 (SPARC) is installed	2009-01-09	cpe:/o:sun:sunos:5.8::sparc
oval:org.mitre.oval:def:6110	V	Windows Search Parsing Vulnerability	2009-01-05	CVE-2008-4269
oval:org.mitre.oval:def:6098	V	Word RTF Object Parsing Vulnerability	2009-01-05	CVE-2008-4027
oval:org.mitre.oval:def:6096	V	Word RTF Object Parsing Vulnerability	2009-01-05	CVE-2008-4028
oval:org.mitre.oval:def:5982	V	Word Memory Corruption Vulnerability	2009-01-05	CVE-2008-4837
oval:org.mitre.oval:def:5952	V	Word RTF Object Parsing Vulnerability	2009-01-05	CVE-2008-4031
oval:org.mitre.oval:def:5934	V	Word Memory Corruption Vulnerability	2009-01-05	CVE-2008-4024
oval:org.mitre.oval:def:5863	V	Windows Saved Search Vulnerability	2009-01-05	CVE-2008-4268
oval:org.mitre.oval:def:5808	V	Excel Global Array Memory Corruption Vulnerability	2009-01-05	CVE-2008-4266
oval:org.mitre.oval:def:5807	V	Word Memory Corruption Vulnerability	2009-01-05	CVE-2008-4026
oval:org.mitre.oval:def:5737	V	Word RTF Object Parsing Vulnerability	2009-01-05	CVE-2008-4030
oval:org.mitre.oval:def:5682	V	Word RTF Object Parsing Vulnerability	2009-01-05	CVE-2008-4025
oval:org.mitre.oval:def:5614	V	File Format Parsing Vulnerability	2009-01-05	CVE-2008-4265
oval:org.mitre.oval:def:5556	V	File Format Parsing Vulnerability	2009-01-05	CVE-2008-4264

Save XML

BACK TO TOP

Slika 4. Primjer izmjene OVAL definicija

Preuzimanje trenutne inačice OVAL repozitorija moguće je preko navedene web stranice:

http://oval.mitre.org/rep-data/index.html

5.4. Trenutna inačica OVAL prevodioca

Najnovija inačica 5.5 objavljena je 10. listopada 2008.g.

Dostupan je za operacijske sustave:

- Linux,
- Vista,
- Win2K,
- WinXP.

Za preuzimanje potrebno je posjetiti slijedeću web stranicu:

http://sourceforge.net/project/showfiles.php?group_id=215469

6. Vlasništvo i financiranje

6.1. Inicijatori i suradništvo

OVAL standard razvila je MITRE korporacija, neprofitabilna organizacija koja se bavi radom za javno dobro. Organizacija kombinira informatičke tehnologije kako bi razvila inovativna rješenja. Rad MITRE organizacije je fokusiran unutar tri FFRDS (eng. Federally Funded Research and Development Centers) centra. Više informacija o njihovom radu moguće je pronaći na web stranici korporacije:

http://www.mitre.org/about/index.html

Osim navedene korporacije, veliku ulogu u razvoju standarda ima OVAL zajednica, koju čine članovi foruma:

- OVAL jezika,
- OVAL repozitorija.

Detaljnije informacije dostupne na web stranici:

http://oval.mitre.org/community/index.html

Također, u razvoju OVAL jezika sudjeluje i OVAL Board organizacija, savjetničko tijelo koje pruža moderatoru uvid u OVAL standard. Iako je važno imati organiziranu podršku za OVAL standard, OVAL Board organizaciju predvodi jedna osoba pa njihov utjecaj zaista čini razliku.

Odgovornost organizacije je suradnja s moderatorom i zajednicom kako bi definirali OVAL standard, dali uvid u strategiju razvoja te podržali OVAL standard u zajednici.

Svaki član ima slijedeće zadatke:

- Prisustvovati sastancima (bar telefonski),
- Pružiti uvid u razvoj strategije,
- Aktivno pratiti raspravu i razvoj na listi,
- Pružiti stručne savjete o OVAL standard zajednici,
- Potražiti mogućnosti predstavljanja OVAL standard zajednici (i u svojim proizvodima).

Jedna organizacija može imati najviše dva predstavnika kao člana OVAL Board organizacije. Popis trenutnih članova, aktivnosti i sl., moguće je pronaći na web stranici:

http://oval.mitre.org/community/board/index.html

OVAL zajednica surađuje s mnogim organizacijama i pojedincima koji pridonose razvoju. Slika 5 prikazuje popis organizacija i pojedinaca koji su imali najveći utjecaj.

Organizacije	UKUPNO
Prijava	
Maitreya Security	2883
The MITRE Corporation	941
ThreatGuard, Inc.	850
Hewlett-Packard	369
Secure Elements, Inc.	248
Bastille Linux	244
Opsware, Inc.	76
Lumension Security, Inc.	11
McAfee, Inc.	4
SecPod Technologies	4
Modifikaciranje	
The MITRE Corporation	1908
ThreatGuard, Inc.	416
Opsware, Inc.	270
Centennial Software	186
Maitreya Security	181
Secure Elements, Inc.	150
Bastille Linux	94
Hewlett-Packard	94
BigFix, Inc	73
GFI Software	60

Pojedinci		UKUPNO
Prijava		
Thomas R. Jones	Maitreya Security	2883
Robert L. Hollis	ThreatGuard, Inc.	850
Jay Beale	Bastille Linux	244
Sudhir Gandhe	Secure Elements, Inc.	197
Christine Walzer	The MITRE Corporation	175
Michael Wood	Hewlett-Packard	174
Andrew Buttner	The MITRE Corporation	162
Yuzheng Zhou	Hewlett-Packard	145
Harvey Rubinovitz	The MITRE Corporation	142
Tiffany Bergeron	The MITRE Corporation	112
Modifikaciranje		
Jonathan Baker	The MITRE Corporation	909
Robert L. Hollis	ThreatGuard, Inc.	416
Christine Walzer	The MITRE Corporation	268
Matthew Wojcik	The MITRE Corporation	243
John Hoyland	Centennial Software	182
Andrew Buttner	The MITRE Corporation	181
Thomas R. Jones	Maitreya Security	181
Jeff Cheng	Opsware, Inc.	175
Ingrid Skoog	The MITRE Corporation	128
Jay Beale	Bastille Linux	94

Slika 5. Utjecaj organizacija i pojedinaca na razvoj OVAL jezika

6.2. Financiranje

Budući da je MITRE korporacija neprofitabilna organizacija, financiranje razvoja OVAL standarda provodi US-CERT (eng. United States Computer Emergency Readiness Team) organizacija. US-CERT je dio Ministarstva za državnu sigurnost SAD – a (eng. U.S. Department of Homeland Security).

Financiranje se provodi zbog dobiti zajednice te prikupljanja zbirke sadržaja o sigurnosti i administraciji sustava stručnjaka širom svijeta.

Poveznice preko kojih je moguće saznati više informacija o:

US-CERT organizaciji - http://www.us-cert.gov/aboutus.html
Ministarstvu za državnu sigurnost SAD-a - http://www.dhs.gov/index.shtm

7. Uporaba i doprinos

7.1. Način korištenja

OVAL jezik je jednostavna reprezentacija ispravnih vrijednosti povezanih s komponentama sustava. Primjeri ispravnih vrijednosti:

„inačica datoteke je 3.5.1“
„vrijednost registratora je 10“

U nastavku dokumenta objašnjeno ja kako ove ispravne vrijednosti mogu biti prikazane u OVAL definicijama. Ovaj opis namijenjen je korisnicima kako bi razumjeli strukturu OVAL definicija.

7.1.1. Primjer *„Hello World“*

„Hello World“ primjer je popularni primjer korišten pri upoznavanju raznih programskih jezika. Pokretanjem „Hello World“ primjera ispisuje se tekst *„Hello World“* na zaslon.

Kako bi se korisnici upoznali s radom OVAL jezika prikazan je jednostavan primjer pisanja definicije koja provjerava da li je vrijednost registra operacijskog sustava Windows (*'HKEY_LOCAL_MACHINE\SOFTWARE\oval\example'*) upravo *„Hello World“*.

Prvi korak u stvaranju definicije je stvaranje OVAL testa koji definira registar i vrijednost koju želimo ispitati. Kada je test jednom napravljen, definicija zatvara taj test u meta podatke.

7.1.2. Test registra

Test u OVAL jeziku koristi se za provjeru vrijednosti određenih atributa povezanih sa zadanim objektom. Struktura OVAL testa uspoređuje referencu zadanog objekta (u danom primjeru registra) s referencom vrijednosti koju provjeravamo.

Svakom testu dodjeljuje se ID vrijednost koja ga jednoznačno određuje. Atribut za provjeru (eng. check attribute) pomaže pri određivanju veze između objekta i stanja. U navedenom primjeru taj atribut ima vrijednost *„all“*, što označava da ce test biti istinit ako SVE vrijednosti registra sustava koje odgovaraju deklaraciji objekta imaju zadanu vrijednost. Kod zadanog primjera samo jedan registar ima vrijednost koja se podudara s objektom, a provjerava se da li ima vrijednost *„Hello World“*.

```
<registry_test id="oval:tutorial:tst:1" check="all">

        <object object_ref="oval:tutorial:obj:1"/>
        <state state_ref="oval:tutorial:ste:1"/>

</registry_test>
```

7.1.3. Objekt registra

Svaki test u OVAL jeziku treba imati jedan ili više objekata za provjeru. Objekti su zapravo „predmeti“ (datoteke, korisnici, registri i sl.) na sustavu kojeg ocjenjujemo. Ti objekti su dijelovi sustava kojeg testiramo.

Za definiranje registratora u OVAL jeziku, potrebno je stvoriti *„registry_object“*, jednostavne XML podatke koji ga jednoznačno identificiraju. U *„Hello World“* primjeru potrebno je kreirati slijedeći objekt:

```
<registry_object id="oval:tutorial:obj:1">

        <hive>HKEY_LOCAL_MACHINE</hive>
        <key>SOFTWARE\oval</key>
        <name>example</name>

</registry_object>
```

7.1.4. Stanje registra

Kada je jednom definiran objekt, slijedeći korak je izražavanje ispravnog stanja objekta (eng. TRUE) za potrebe testiranja. U zadanom primjeru treba stvoriti *„registry_state“* i zadati provjeru da pronađeni registar ima vrijednost *Hello World* (eng. "check that the registry we identified has a value of Hello World").

```
<registry_state id="oval:tutorial:ste:1">

        <value>Hello World</value>

</registry_state>
```

7.1.5. Definicija

Definicija je središnji dio OVAL jezika, jer služi kao referenca aplikacijama tijekom ocjenjivanja sustava. Svrha definicija je kombinirati jedan ili više testova koristeći logički operator AND ili OR. One „omotaju“ meta podatke oko testova kako bi omogućile povratnu informaciju o radnjama korisnicima.

```
<definition id="oval:tutorial:def:1">

        <metadata>...</metadata>
        <criteria>...</criteria>

</definition>
```

7.1.6. Meta podaci

Skupina meta podataka povezana je sa svakom definicijom kako bi pružila tekstualni opis onoga što se provjerava i kako se treba koristiti. Jedini zahtijevani dio meta podataka su naslov i opis. Dodatni meta podaci mogu biti dodani ako se traži.

```
<metadata>
        <title>Hello World Example</title>
        <description>
                This definition is used to introduce the OVAL
Language to individuals
                interested in writing OVAL Content.
        </description>
</metadata>
```

7.1.7. Kriterij

Kriterij OVAL definicije označava što se testira, a sadrži sve individualne testove i spaja ih u jednu cjelinu pomoću AND ili OR operatora. Ovo omogućuje individualno pisanje definicije za npr. „ispitaj postojanje datoteke AND vrijednost registra je 10“. Naravno, naš primjer samo provjerava jednostavan registar pa će kriterij sadržati samo jedan test. Primjer ispod prikazuje kako treba zadati kriterij za „*Hello World*“ primjer.

```
<criteria>
        <criterion test_ref="oval:tutorial:tst:1"
        comment="the value of the registry key equals Hello
World"/>
</criteria>
```

Svaki kriterij sadrži individualne naredbe koje označuju jedan test. Konačni test je pisan posebno i referenciran ID vrijednošću sa „*test_ref*“ atributom. U navedenom primjeru traži se test *oval:tutorial:tst:1*, a komentar (eng. comment) objašnjava što test treba napraviti.

7.1.8. Potpuna datoteka definicije

Nakon stvaranja svih dijelova, moguće je kombinirati ih u datoteku OVAL definicije.

```
<oval_definitions>

          <definitions>

                    <definition id="oval:tutorial:def:1">

                              <metadata>
                                        <title>Hello World Example</title>
                                        <description>
                    Definicija je namijenjena upoznavanju korisnika
               s pisanjem OVAL Sadržaja u OVAL jeziku.
                              </metadata>

                              <criteria>
                                        <criterion test_ref="oval:tutorial:tst:1"
                                        comment="the value of the registry key equals Hello
                                        World"/>
                              </criteria>

                    </definition>

          </definitions>

          <tests>

                    <registry_test id="oval:tutorial:tst:1" check="all">
                              <object object_ref="oval:tutorial:obj:1"/>
                              <state state_ref="oval:tutorial:ste:1"/>
                    </registry_test>

          </tests>

          <objects>

                    <registry_object id="oval:tutorial:obj:1">
                              <hive>HKEY_LOCAL_MACHINE</hive>
                              <key>SOFTWARE\oval</key>
                              <name>example</name>
                    </registry_object>

          </objects>

          <states>

                    <registry_state id="oval:tutorial:ste:1">
                              <value>Hello World</value>
                    </registry_state>

          </states>

</oval_definitions>
```

7.2. Kako se pridružiti?

OVAL zajednica poziva sve prodavače programa, ljude koji se bave informacijskom sigurnošću, programere te druge korisnike uključene u sigurnost računala da se pridruže OVAL forumima:

- OVAL forum repozitorija – javni forum za raspravu o novim i ranijim sadržajima OVAL repozitorija, kao i ranjivostima i konfiguracijskim problemima koji se pojavljuju u definicijama.
- OVAL forum za razvoj – javni forum za raspravu o OVAL jeziku, kao i posebnim temama kao što su problemi OVAL implementacije i međudjelovanje OVAL jezika s drugim alatima.
- OVAL forum za posredništvo – javni forum za raspravu i razvoj standardnog jezika koji utječe na znanje OVAL zajednice i iskustvo prikupljeno razvojem OVAL jezika.

Prijavnicu je moguće ispuniti na stranici:

http://oval.mitre.org/community/registration.html

Također, moguće je poslati zahtjev za uključivanjem u OVAL Board organizaciju na slijedeću adresu elektroničke pošte:

oval@mitre.org

Pri tome, svi potencijalni članovi OVAL Board organizacije prvo moraju biti članovi OVAL zajednice.

Osim toga, svaki pojedinac ili organizacija može prijaviti novu definiciju, a detaljne upute o samom procesu dostupne su na slijedećoj web stranici:

http://oval.mitre.org/repository/about/submission.html

Napomena: SVI članovi moraju se pridržavati određenih propisa koje je moguće pronaći preko navedene poveznice:

http://oval.mitre.org/oval/about/privacy_policy.html

8. Očekivanja u budućnosti

8.1. Očekivanja autora

Autori i OVAL zajednica planiraju razvoj inačice 6.0 OVAL jezika. Nova inačica treba donijeti razne izmjene pa će zahtijevati i razvoj alata.

Neke planirane novosti u inačici 6.0:

- Dopuštanje korištenja filtara na razini grupe, a ne samo na razini objekta,
- Omogućiti uniformno stavljanje referenci shemama,
- Uvesti način povezivanja sadržaja sa vanjskim lokacijama,
- Potrebno dodati nabrajanje (eng. enumeration) za tipove UNIX datoteka,
- Dopuštanje testovima da zauzimaju višestruka stanja,
- Ukloniti standardna prava SYNCHRONIZE pristupa iz testova registra,
- Dodati novi test za Windows postavke (eng. inheritence settings),
- Uvesti odabir strukture u objekte,
- Dodati novi test za dozvole dijeljena na korisničkoj razini,
- Dodati podršku za naredbe koje vraćaju višestruke vrijednosti *sql*, *wmi* i *activedirectory* testova,
- Promijeniti tip *epoch* entiteta *rpminfo_test* testa iz *string* u *int*,
- Omogućiti korištenje *xml:lang* za komentare,
- Dodati atribute za osjetljivost na velika i mala slova,
- Dodati novi test za Apache konfiguraciju,
- Dodati atribut koji podržavaju redoslijed elemenata za funkcije poput *concat,*
- Dodati operacije dijeljenja i spajanja računskim funkcijama,
- Ostvariti podršku za registar koji sadrže putanju i ime datoteke,
- Uskladiti testove i imena elemenata.

Osim planiranja nove inačice, MITRE organizacija surađuje s NIST institutom SAD-a (eng. U.S. National Institute of Standards and Technology) kako bi zamijenila program OVAL kompatibilnosti sa dva neovisna, ali komplementarna programa:

- Program OVAL uvođenja (eng. OVAL Adoption Program) kojim će upravljati MITRE organizacija,
- Program SCAP (eng. Security Content Automation Protocol) provjere kojim će upravljati NIST institut.

Taj novi program omogućit će MITRE organizaciji fokusiranje na napredak OVAL standard, kao i na podršku organizacijama koje prihvaćaju OVAL standard. 1. travnja 2009. počinje testiranje svih alata sa popisa OVAL kompatibilnih proizvoda pomoću SCAP testa, kako bi se napravio novi popis (alata koji su prošli provjeru). Predviđeno trajanje ovog programa testiranja je godinu dana. Detaljan opis programa moguće je pronaći u slijedećem dokumentu:

http://oval.mitre.org/adoption/Adoption_and_Validation_August2008.pdf

8.2. Očekivanja javnosti

Zahvaljujući širokom skupu alata koje razvijaju stručnjaci za sigurnost, korisnicima je omogućena velika fleksibilnost pri izboru i primjeni alata. Iako postoji dostupno mnogo komercijalnih i besplatnih proizvoda, razvoj standardnih definicija omogućuje prilagodbu alata za određene poslove ili razvoj novih alata, kao i njihovu međusobnu suradnju.

Vlasti su već primijetile ovu vrijednost OVAL standard pa se vjeruje da će sve više organizacija početi s uporabom navedenog standarda. Ipak, svi proizvodi koji zadovoljavaju OVAL standard moraju proći

SCAP test, koji se oslanja na standardu za imenovanje ranjivosti i konfiguracije u aplikacijama i sustavima. Ovo ukazuje na poticanje agencija, prodavača alata i autora na razvoj sigurnijih proizvoda. Zbog toga se očekuje veća uporaba svih alata koji zadovoljavaju određene sigurnosne propise.

Daljnjim razvojem standarda, sigurnosni proizvodi će povećati kvalitetu i pružiti timovima za sigurnost potrebne sadržaje za razvoj alata kako bi osigurali sigurnost infrastrukture, bez obzira na složenost mreža i aplikacija.

9. Zaključak

Razvoj OVAL standarda omogućio je uvođenje standardnog oblika zapisa ranjivosti i konfiguracijskih problema, što donosi veliku prednost kako proizvođačima raznih sigurnosnih alata, tako i samim korisnicima. Proizvođači alata dobili su mogućnost fokusiranja na razvoj boljih značajki svojih proizvoda, ne vodeći računa o učenju raznih jezika za opis ranjivosti. Zahvaljujući jedinstvenom OVAL jeziku korištenom u svim definicijama proizvođači imaju mogućnost poboljšanja funkcionalnosti proizvoda i razvoja kvalitetnijih alata. Prednost korisnika je mogućnost vlastitog testiranja određenog proizvoda bez zahtjeva za velikim znanjem jezika. Nakon otkrivene pogreške korisnici mogu potražiti odgovarajuća programska rješenja ili samostalno pokušati ukloniti problem. Osim toga, postojanje gotovih, javno dostupnih OVAL definicija, pruža svim korisnicima mogućnost njihova preuzimanja te izmjene na način koji njima odgovara. Pri tome, svi korisnici imaju mogućnost uključivanja u razvoj jezika i definicija, što dovodi do velike popularnosti i raširenosti ovog standarda.

Budući razvoj ukazuje na izdavanje poboljšanje inačice OVAL jezika, kao i na proširivanje OVAL repozitorija zahvaljujući stalnom dodavanju novih te ispravljanju postojećih OVAL definicija. Također, proizvođače programskih rješenja potiče se na pravilnu primjenu OVAL standarda, kako bi zadovoljili uvjete SCAP testa te dobili oznaku OVAL kompatibilnog alata.

10. Reference

[1] OVAL standard, http://oval.mitre.org/index.html, siječanj, 2009.

[2] OVAL, http://en.wikipedia.org/wiki/Open_Vulnerability_and_Assessment_Language, siječanj, 2009.

[3] OVAL FAQ, http://oval.mitre.org/oval/about/faqs.html, siječanj, 2009.

[4] OVAL jezik, http://oval.mitre.org/language/index.html, siječanj, 2009.

[5] OVAL repozitorij, http://oval.mitre.org/repository/index.html, siječanj, 2009.

[6] OVAL prevodilac, http://sourceforge.net/projects/ovaldi/, siječanj, 2009.

[7] OVAL kompatibilnost, http://oval.mitre.org/compatible/index.html, siječanj, 2009.

[8] OVAL Bord organizacija, http://oval.mitre.org/community/board/index.html, siječanj, 2009.

[9] OVAL zajednica, http://oval.mitre.org/community/index.html, siječanj, 2009.

[10] MITRE korporacija, http://www.mitre.org/, siječanj, 2009.

[11] US-CERT, http://www.us-cert.gov/, siječanj, 2009.

[12] US-CERT, http://www.us-cert.gov/oval.html, siječanj, 2009.