CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Izvori informacija o sigurnosnim ranjivostima

NCERT-PUBDOC-2010-05-299

Nacionalni CERT

u suradnji s

LSS

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

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

Nacionalni 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

Unatoč velikom trudu sigurnosnih organizacija, proizvođača, timova za rješavanje incidenata te raznih vladinih organizacija, gotovo svaki programski proizvod sadrži brojne sigurnosne ranjivosti. Radi se o nekom nedostatku u programu ili sustavu koji zlonamjernom korisniku može pružiti mogućnost narušavanja sigurnosti sustava ili informacija. Nedostatak može uključivati pogrešku u kodu, implementaciji, rukovanju podacima, protokolima i mnoge druge probleme.

Ideja o praćenju sigurnosnih ranjivosti javila se još prije više od pola stoljeća, kada se počelo s formiranjem prvih organizacija s takvom zadaćom. Postupak praćenja ranjivosti uključuje njeno pronalaženje, analizu, dojavu proizvođaču te javnu objavu prikupljenih informacija. Tokom povijesti uvedeni su razni identifikatori sigurnosnih ranjivosti (CVE, Bugtraq, OSVDB i dr.), tj. jedinstvene oznake pridruženje jednoj ranjivosti radi sustavnog praćenja i raspoznavanja. Svaka sigurnosna organizacija koja je provodila samostalno praćenje i analizu definirala je poseban identifikator koji označava ranjivosti u njihovim bazama. Kako bi se osigurala bolja suradnja i povezanost raznih izvora podataka o ranjivostima, jedan se standard istaknuo kao referentni. Radi se o CVE (eng. *Common Vulnerabilities and Exposures*) standardu i bazi podataka kojom upravlja organizacija Mitre. Osim spomenute baze sigurnosnih ranjivosti, postoje još brojne druge, poput baza organizacija Secunia, SecurityFocus te CERT. Svaka od navedenih ima isti cilj - biti središnji izvor podataka o sigurnosnim prijetnjama.

Ovaj dokument donosi kratki uvod u značenje sigurnosnih ranjivosti i procesa njihova praćenja. Zatim je dan sustavan pregled svih identifikatora ranjivosti uz opis njihova značenja i uporabe. Slijedi detaljan opis baza podataka koje predstavljaju izvore informacija o sigurnosnim ranjivostima. Pred kraj dokumenta predstavljeni su problemi s kojim se susreću organizacije pri održavanju takvih baza te očekivanja u budućnosti.

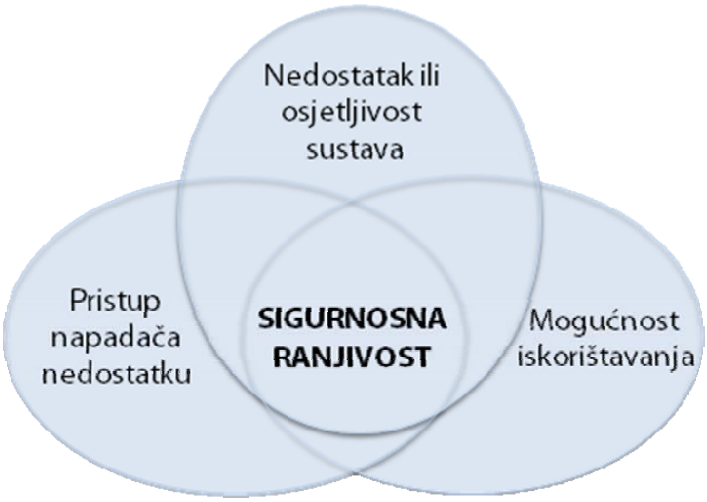
2. Sigurnosna ranjivost

2.1. Značenje i obilježja

Izraz sigurnosna ranjivost opisuje nedostatak koji napadaču omogućava da ugrozi sigurnost informacija (eng. *information assurance*) nekog sustava.

Može se definirati kao presjek tri elementa (Slika 1):

- osjetljivosti sustava ili nedostatka,
- pristupa napadaču do nedostatka,
- sposobnosti napadača da iskoristi nedostatak.



Slika 1. Sigurnosna ranjivost

Kako bi napadač iskoristio ranjivost, on mora poznavati bar jedan alat ili tehniku kojom je to moguće izvesti. Svaka ranjivost s jednim ili više poznatih instanci potpuno implementiranih napada klasificira se kao iskorištena ranjivost (eng. *exploit*). Vrijeme od trenutka kada je sigurnosna rupa uvedena u proizvod u razvoju do njenog uklanjanja, izdavanja sigurnosne nadogradnje ili onemogućavanja napadača naziva se prozor ranjivosti.

Postoji nekoliko obilježja koja određuju razinu ranjivosti:

- **složenost** – kod velikih, složenih sustava povećana je vjerojatnost nedostataka i mogućih točaka neautoriziranog pristupa;
- **uporaba poznatih alata** – prilikom korištenja dobro poznatih kodova, programa, operacijskih sustava i/ili sklopovlja napadaču je jednostavnije pronaći način za iskorištavanje ranjivosti;
- **povezanost** – korištenje više fizičkih veza, prava, priključaka, protokola i usluga kojima se može pristupiti povećava ranjivost sustava;
- **upravljanje lozinkama** – sustav je izložen napadima ukoliko korisnici koriste slabe lozinke, pohranjuju ih na nesigurna mjesta te koriste iste lozinke za više programa i aplikacija;
- **osnovni dizajn operacijskog sustava** – ako dizajner operacijskog sustava uvede pogrešnu politiku za upravljanje pravima korisnika/programa može doći do nedozvoljenog povećanja prava na sustavu;
- **pretraživanje web stranica** – web stranice mogu sadržavati razne zlonamjerne programe koji se automatski instaliraju na računalo korisnika prilikom posjete tih stranica;
- **pogreške u programima** – svaka neispravljena pogreška u razvoju nekog programa može napadaču omogućiti pokretanje raznih napada;

- **neprovjeravanje korisničkih unosa** – ako program pretpostavlja da su svi korisnički unosi ispravni i sigurni, takvu situaciju napadač može iskoristiti za pokretanje napada, primjerice, umetanjem SQL nizova.

2.2. Način praćenja sigurnosnih ranjivosti

Proces praćenja sigurnosne ranjivosti počinje njenim otkrivanjem, a uključuje sljedeće strane:

- **pronalazač** – sigurnosni istražitelj, korisnik ili neka druga osoba/organizacija koja je otkrila sigurnosnu ranjivost,
- **prodavatelj** – osoba, organizacija ili tvrtka koja razvija proizvod ili je zadužena za njegovo održavanje,
- **koordinator** – opcionalni učesnik koji sadrži posredničke poslužitelje za pronalazača ili prodavatelja, a pruža tehničku pomoć ili obavlja neku drugu funkciju u procesu otkrivanja ranjivosti,
- **arbitar** – opcionalni učesnik koji rješava sukobe između pronalazača i prodavatelja.

Proces praćenja ranjivosti odvija se kroz faze prikazane na Slika 2:

1. **Otkrivanje** – korisnik/organizacija pronalazi potencijalni nedostatak.
2. **Obavještavanje** – pronalazač obavještava prodavača o potencijalnom nedostatku, a on potvrđuje da je primio obavijest.
3. **Istraga** – proizvođač pokreće istragu kako bi provjerio tvrdnje o mogućem nedostatku (može surađivati s otkrivačem).
4. **Rješavanje** – ako se potvrdi nedostatak, prodavatelj razvija programsku nadogradnju koja otklanja nedostatak.
5. **Objavljivanje** – prodavatelj i pronalazač zajedno javno objavljuju informacije o ranjivosti i rješenju.

Slika 2. Koraci u praćenju sigurnosne ranjivosti

2.3. Povijest sistematičnog praćenja ranjivosti

U nastavku su kronološkim redoslijedom prikazan počeci praćenja sigurnosnih ranjivosti u raznim organizacijama.

- Godine 1958. osnovana je organizacija MITRE na inicijativu sudionika SAGE (eng. *Semi-Automatic Ground Environment*) projekta, automatiziranog sustava za praćenje i presretanje aviona.
- U studenom 1988. godine osnovan je centar CERT/CC kao odgovor na napad Morrisovim crvom.
- Godine 1989. osnovana je organizacija CIAC koja je 2008. godine preimenovana u DOE-CIRC.
- 5. studenog 1993. godine Scott Chasin je osnovao Bugtraq zbog tadašnjeg stanja sigurnosti Internet infrastrukture. Od sredine 1999. godine u vlasništvu je organizacije „SecurityFocus".
- Godine 1999. stvorena je CVE baza podataka (u vlasništvu korporacije Mitre).
- Organizacija SecurityFocus osnovana je 1999. godine, ali nakon tri godine dolazi u vlasništvo korporacije Symantec.
- Na sigurnosnim konferencijama Black Hat i Defcon, 1. svibnja 2002. godine, uvedene su dvije nove usluge među kojima se našla i baza sigurnosnih ranjivosti OSVDB. Sljedeće godine na konferenciji Defcon odlučeno je predstaviti bazu javnosti.
- Secuniu je, 2002. godine, osnovao tim profesionalnih menadžera, prodavača, IT stručnjaka i programera pod vodstvom Nielsa Henrika Rasmussena.

- U rujnu 2003. godine osnovana je organizacija US-CERT kako bi surađivala s centrom CERT/CC u analiziranju i sprječavanju napada .

3. Identifikatori ranjivosti

3.1. CVE identifikator

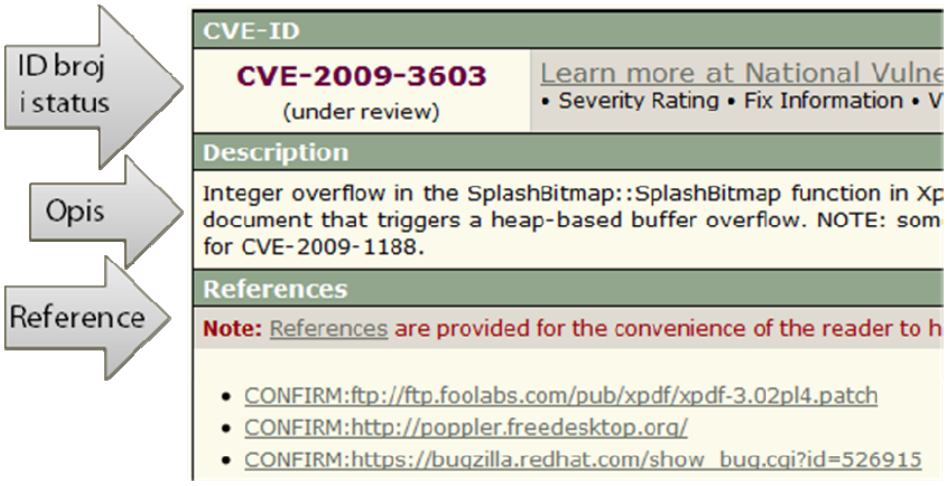
CVE (eng. *Common Vulnerabilities and Exposures*) je besplatni rječnik osnovnih imena (tj. CVE identifikatora) za javno poznate sigurnosne ranjivosti. CVE identifikatori omogućuju jednostavno dijeljenje podataka preko raznih baza podataka o mrežnoj i računalnoj sigurnosti te pružaju temelj za provjeru konvergencije nekog alata. Omogućuje uporabu jedne oznake za jednu ranjivost ili njeno iskorištavanje te jednog standardiziranog opisa za svaku ranjivost ili njeno iskorištavanje.

Svaki CVE identifikator uključuje (Slika 3):

- CVE identifikacijski broj (npr. CVE-2010-0067),
- status,
- kratki opis sigurnosne ranjivosti ili načina njenog iskorištavanja,
- dodatne reference (npr. sigurnosna preporuka).

Postoje dva statusa identifikatora, a to su:

1. „entry“ – identifikator je prihvaćen na CVE listu
2. „candidate“ – identifikator je u procesu provjere za uključenje u listu.



Slika 3. Pretraživanje ranjivosti po CVE ID
Izvor: CVE

3.1.1. Kreiranje identifikatora

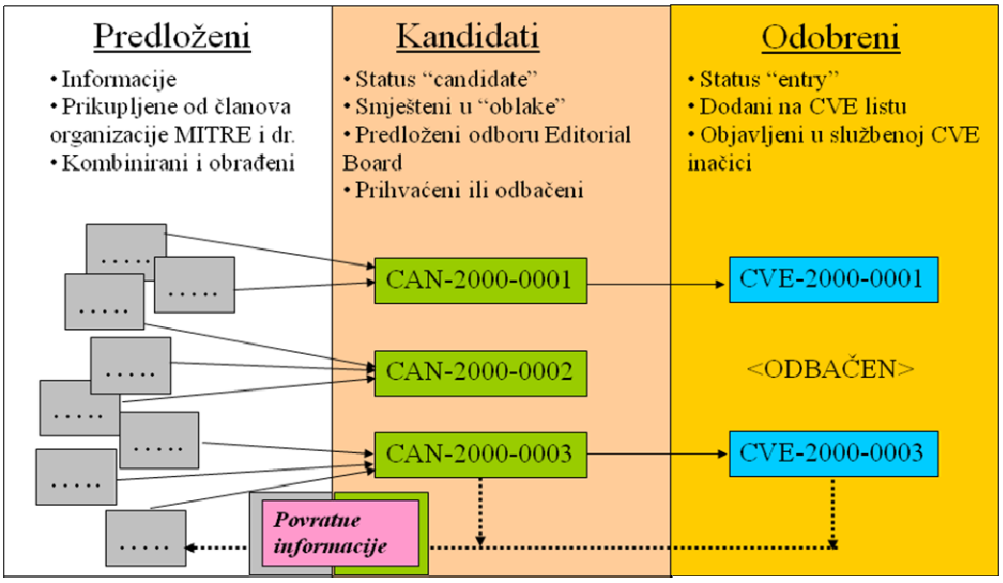
Proces kreiranja CVE identifikatora počinje s otkrivanjem potencijalnih sigurnosnih ranjivosti ili načina njihova iskorištavanja. Osoba koja je otkrila nedostatak zahtjeva jedan ili više „candidate“ brojeva. Odjel CVE CNA (eng. *Candidate Numbering Authority*) dodijeli informacijama CVE broj („candidate“). CVE CNA je skup više proizvođača sigurnosnih proizvoda (Apple, Oracle, FreeBSD, Ubuntu Linux, Microsoft Corporation i dr.), koordinatora (CERT/CC) te istražitelja (Secunia). Predsjedničko mjesto zauzela je organizacija MITRE. Nakon dodjele broja, organizacija MITRE kreira mjesto za opis ranjivosti na web stranici. Osoba koja je zahtijevala broj mora ga proslijediti svim stranama uključenim u otkrivanje ranjivosti te ga uključiti u sigurnosnu preporuku. Nakon javne objave obavještava se organizacija MITRE koja objavljuje detalje na mjestu rezerviranom na CVE web stranici te predstavlja kandidata odboru CVE Editorial Board. Ukoliko odbor prihvati kandidata, mijenja se status u „entry“ te se osvježavaju informacije.

Cjelokupni postupak može se podijeliti u tri faze (prikazano na Slika 4):

1. Predlaganje (eng. *submission*) – organizacija MITRE ima tim čiji je osnovni zadatak analizirati, istraživati i obrađivati primljene prijave o ranjivostima iz raznih izvora podataka. Vođa tima je CVE urednik (eng. *CVE Editor*) koji je odgovaran za sav CVE sadržaj.
    a. Faza konverzije (eng. *conversion phase*) – tim prikuplja informacije iz raznih izvora te ih pretvara u prijedloge predstavljene u standardiziranom obliku kako bi se mogli automatski obrađivati. Svaki prijedlog uključuje jedinstveni identifikator koji koristi neki izvor podataka.
    b. Faza uklapanja (eng. *matching phase*) – nakon faze konverzije, svaki prijedlog se automatski uspoređuje s ostalim prijedlozima, kandidatima i prihvaćenim kandidatima. Temelji se na ključnim riječima koje se izvuku iz opisa, referenci i naziva. Ova tehnika nije u potpunosti pouzdana pa se uzorci najbliži ciljanom (npr. 10 njih) predaju timu koji identificira koji prijedlozi opisuju isti problem. Rezultat faze uklapanja su prijedlozi grupirani tako da opisuju jednu ranjivost ili skupinu blisko povezanih ranjivosti.
    c. Faza pročišćavanja (eng. *refinement phase*) – svakom članu tima dodijeli se 20 ili više grupa prijedloga. Članovi analiziraju grupe i određuju koji prijedlog najbolje identificira neki postojeći CVE identifikator. Tada se obavlja samo proširenje identifikatora dodatnim referencama. Ukoliko takvih prijedloga ne postoji, članovi procjenjuju da li treba kreirati novi identifikator sa statusom „*candidate*“. Ako odluče kreirati identifikator moraju definirati opis, provjeriti da li proizvođač zna za ranjivost, odrediti ključne riječi i dodatne informacije (poput dana otkrivanja ranjivosti i sl.). Ova faza predstavlja vrlo zahtjevan i složen dio procesa.
    d. Faza editiranja (eng. *editing phase*) – nakon faze pročišćavanja, CVE urednik pregledava posao analitičara te po potrebi obavlja izmjene. Također, urednik može spojiti grupe koje su obradili različiti članovi tima ako primijeti podudarnosti. Svakoj preostaloj grupi dodjeljuje broj, a svaki izvor podataka prima povratne informacije o dodijeli CVE broja.

   U nekim slučajevima opisane faze je moguće zaobići (npr. ako organizacija rezervira broj kako bi ga uključila u javnu objavu ranjivosti).
2. Kandidati (eng. *Candidates*):
    a. Faza dodjeljivanja (eng. *assignment phase*) – kandidati se stvaraju na jedan od tri načina:
        i. kroz postupak predlaganja,
        ii. rezervacijom brojeva ili
        iii. ubrzanim kreiranjem zbog rizičnog problema (provodi urednik).
    b. Faza predlaganja (eng. *proposal phase*) – urednik organizira kandidate u „oblake“ koji sadrže 20 – 50 kandidata. Za nove ranjivosti, oblaci su obično grupirani prema datumu inicijalne javne objave kandidata. Takvi oblaci predstavljaju se odboru (eng. *Board*) radi provjere i glasovanja.
    c. Faza glasovanja (eng. *voting phase*) – članovi odbora pregledavaju kandidate te provode glasovanje. Kandidati mogu biti prihvaćeni, vraćeni na izmjenu, odbačeni, označeni za potpunu izmjenu te označeni za dodatno pregledavanje.
    d. Faza izmjene (eng. *modification phase*) – kandidat se izmjenjuje prema naputku odbora.
    e. Faza privremene odluke (eng. *interim decision phase*) – CVE urednik određuje kada je pregled kandidata gotov nakon čega odbor mora provesti konačno komentiranje. U ovoj fazi kandidat može biti vraćen u fazu izmjena (ako se zahtjeva dodatno glasovanje).
    f. Faza krajnje odluke (eng. *final decision phase*) – ako CVE urednik odredi da ne postoji više mogućnost izmjene glasanja koje je obavljeno u fazi privremene odluke, odluka postaje konačna. Ukoliko je kandidat prihvaćen, urednik obavještava odbor o njegovu dodavanju u CVE listu te mu dodjeljuje CVE ime. U slučaju da je kandidat odbačen, urednik navodi razlog.
3. Odobreni (eng. *entries*)

a. Faza objavljivanja (eng. *publication phase*) – kandidatu se mijenja status, uklanjaju se zapisi o glasovanju te se ranjivost dodaje u CVE popis.
b. Faza izmjene (eng. *modification phase*) – odobrenog kandidata moguće je izmijeniti dodavanjem opisa ili referenci.



Slika 4. Umetanje novih ranjivosti na CVE listu
Izvor: CVE

3.2. Bugtraq ID

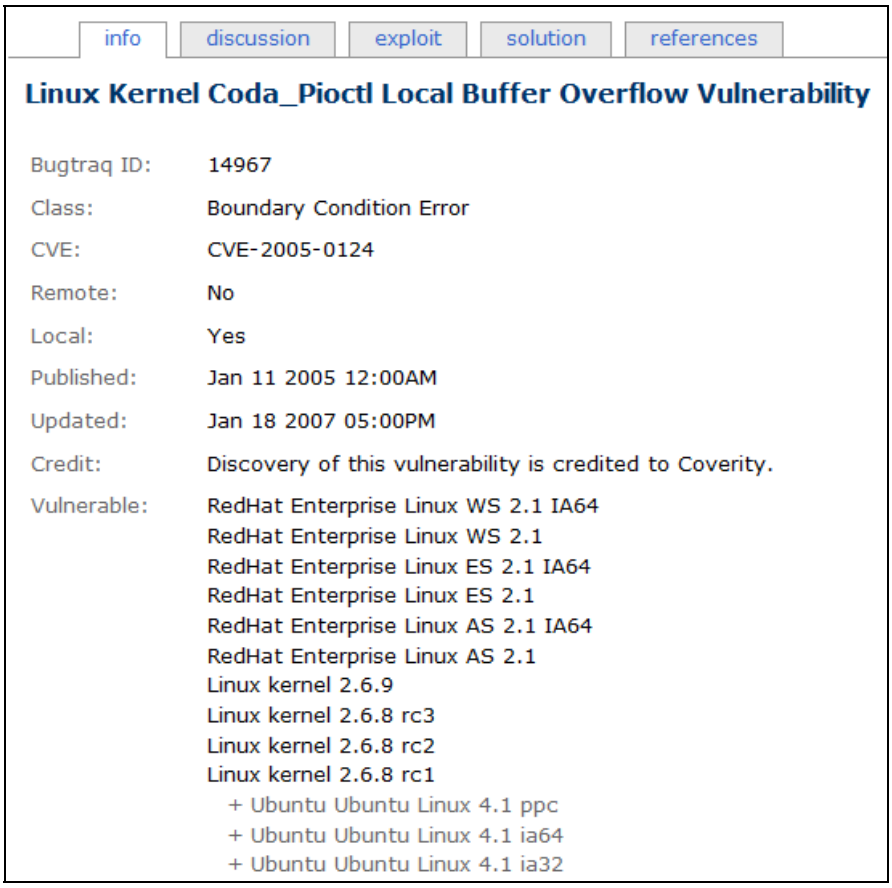
Bugtraq je elektronička *mailing* lista i baza podataka o sigurnosnim problemima, novim raspravama o ranjivostima, obavijestima proizvođača, metodama iskorištavanja te načinu ispravka problema. U počecima je bila namijenjena za objavu ranjivosti bez obzira na znanje proizvođača o ranjivosti.

Svakoj ranjivosti koja se dodaje u bazu pridruži se jedinstvena oznaka pod nazivom „Bugtraq ID". Radi se o broju koji jednoznačno označuje jednu ranjivost, a uz njega slijede dodatne informacije poput:

- klase ranjivosti,
- CVE ID,
- informacije o vrsti napada (udaljeni ili lokalni),
- datuma objave i osvježavanja informacija,
- ranjivih paketa,
- rasprava,
- načina iskorištavanja,
- rješenja,
- referenci.

Primjer jedne ranjivosti upisane u bazu Bugtraq dan je na Slika 5.

Opisani identifikator koristi se za bazu podataka koja se upotrebljava u sigurnosnim preporukama. Razlika u odnosu na CVE identifikator je u tome što CVE predstavlja međunarodnu oznaku koja je besplatna za uporabu te ima ulogu pružiti osnovno ime ranjivostima.



Slika 5. Pretraživanje ranjivosti po Bugtraq ID
Izvor: SecurityFocus

3.3. OSVDB ID

OSVDB (eng. *Open Source Vulnerability Database*) je baza podataka koja sadrži sigurnosne ranjivosti, a uvedena je s ciljem jednostavnije suradnje između poduzeća i/ili korisnika.

Ranjivosti u OSVDB bazi su zapisane preko identifikatora OSVDB ID, jedinstvenog broja dodijeljenog svakoj ranjivosti u bazi. Svakoj ranjivosti može se pristupiti na vrlo jednostavan način preko URL nizova:

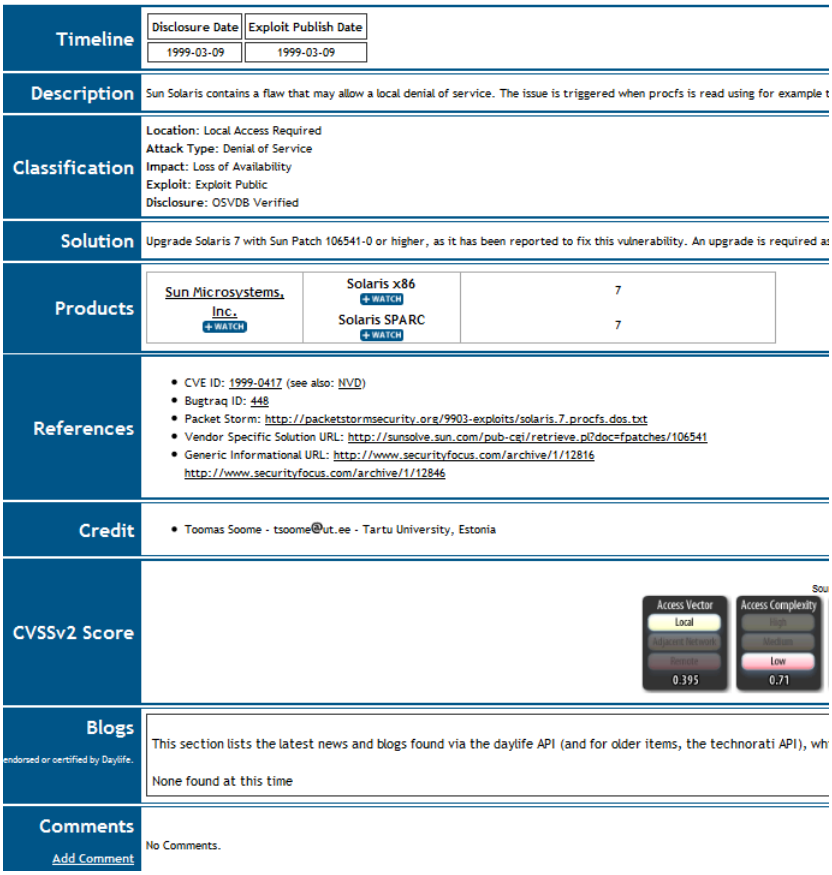
```
http://www.osvdb.org/show/osvdb/XXXX
http://www.osvdb.org/XXXX
```

gdje XXXX predstavlja OSVDB ID.

Prilikom indeksiranja ranjivosti preko opisanog identifikatora korisnik dobije sljedeće informacije:

- datum otkrivanja ranjivosti,
- opis,
- klasifikacije,
- rješenje,
- ugrožene proizvode,
- reference,
- komentare.

Jedan od primjera ranjivosti dan je na Slika 6.



Slika 6. Pretraživanje ranjivosti preko OSVDB ID
Izvor: OSVDB

3.4. Ostali identifikatori

Još neki od identifikatora sigurnosnih ranjivosti navedeni su u nastavku:

- broj CERT preporuke (eng. *CERT Advisory Number*) – sastoji se od oznake godine u kojoj je otkrivena ranjivost te rednog broja (npr. CA-2004-02), a koristi ju organizacija CERT;
- CERT VU broj (eng. *CERT VU Number*) – broj koji jednoznačno označava ranjivost (npr. 619982), a koristi ga organizacija US-CERT;
- broj CIAC preporuke (eng. *CIAC Advisory Number*) – broj preporuke u kojoj je opisana ranjivost (npr. O-084), a koristila ga je organizacije CIAC (trenutno DOE-CIRC);
- XF ID – broj koji jednoznačno određuje ranjivost (npr. 1234), a upotrebljava ga organizacija ISS X-Force;
- ID Secunia preporuke (eng. *Secunia Advisory ID*) – broj koji jednoznačno određuje ranjivost (npr. 10123), a koristi ga organizacija Secunia;
- Security Tracker ID – broj koji jednoznačno određuje ranjivost (npr. 1009695), a upotrebljava ga organizacija Security Tracker;
- Technical Security Advisory ID – niz znakova koji jednoznačno određuju jednu ranjivost (npr. TA04-041A), a koriste se kao oznaka preporuke u organizaciji US-CERT.

4. Poznate baze ranjivosti

4.1. Mitre CVE

Mitre je neprofitabilna, neovisna korporacija koja pruža tehničku podršku vladinim organizacijama. Među brojnim projektima koje razvija, održava i vodi nalazi se i baza podataka o sigurnosnim ranjivostima. Uloga korporacije je uređivanje:

- CVE liste uz pomoć CVE urednika i odbora,
- CVE web stranice,
- CVE programa usklađenosti
- te pružanje neutralnog vodstva kroz proces osiguravanja da CVE služi javnom interesu.

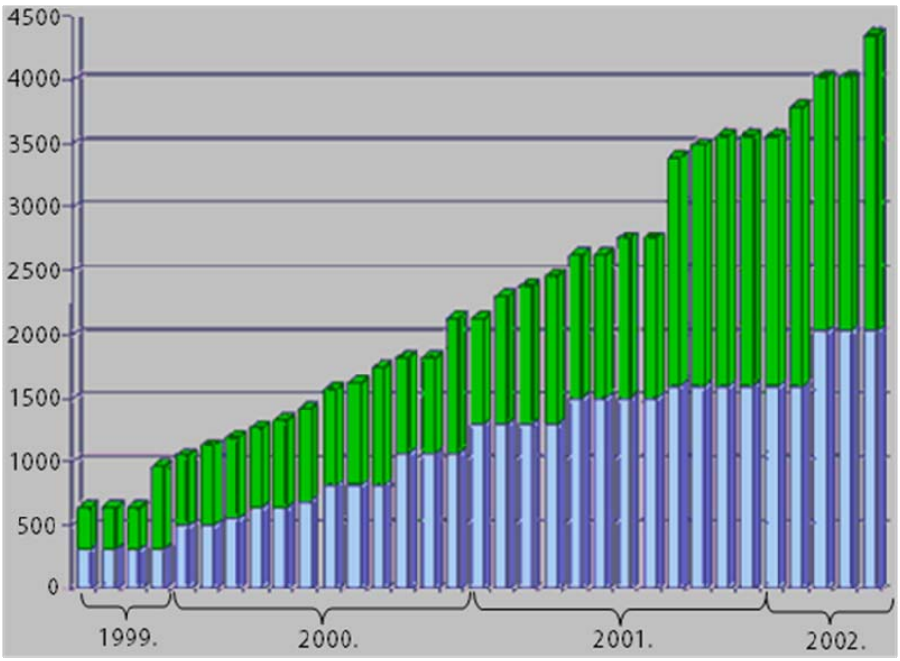
CVE baza podataka razvijena je kako bi se olakšalo dijeljenje podataka o ranjivostima alata i usluga. Mnoge organizacije omogućile su kompatibilnost s CVE standardom te uvele CVE identifikatore u sigurnosne preporuke. Razlikuje se od ostalih baza jer ne sadrži informacije o razini rizika, načinu uklanjanja prijetnji ili detaljnim tehničkim informacijama. Ona pruža samo standardni identifikacijski broj, oznaku statusa, kratki opis i reference na dodatne informacije.

Neke od dobrih karakteristika su:

- sadrži popis svih javno poznatih sigurnosnih ranjivosti,
- dodjeljuje jedinstveni identifikator svakoj ranjivosti,
- pruža osnovni jezik za referenciranje problema,
- olakšava dijeljenje podataka među
    - IDS (eng. *Intrusion Detection Systems*) sustavima,
    - alatima za procjenu ranjivosti,
    - bazama podataka s ranjivostima,
    - istražiteljima i
    - timovima za oporavak od incidenata,
- omogućuje poboljšanje rada sigurnosnih alata,
- neovisna je,
- javno dostupna,
- usmjerenja na ranjivosti umjesto na napade,
- rezultat rada skupine proizvođača sigurnosnih alata i raznih sigurnosnih organizacija.

Zapisi u bazi podataka moraju osigurati konzistentnost te omogućiti jednostavan pregled i dohvat informacija korisnicima. Odluke o sadržaju (eng. *content decision*) su smjernice koje osiguravaju kreiranje CVE identifikatora u konzistentnom stanju i čine ih neovisnim o autoru. Pri tome, ICD (eng. *inclusion content decision*) specificira da li ranjivost treba ući u CVE, a ACD (eng. *abstraction content decision*) definira razinu apstrakcije opisa ranjivosti.

Prva inačica baze sadržavala je samo 321 zapis ranjivosti. Ubrzo se pokazalo da broj ranjivosti raste ubrzanim tempom. Tokom 2000. godine taj broj je dosegao preko 2000 ranjivosti, a početkom 2002. se udvostručio. Rast broja ranjivosti upisanih u CVE bazu prikazan je na Slika 7.



Slika 7. Rast broja ranjivosti u CVE bazi
Izvor: CVE

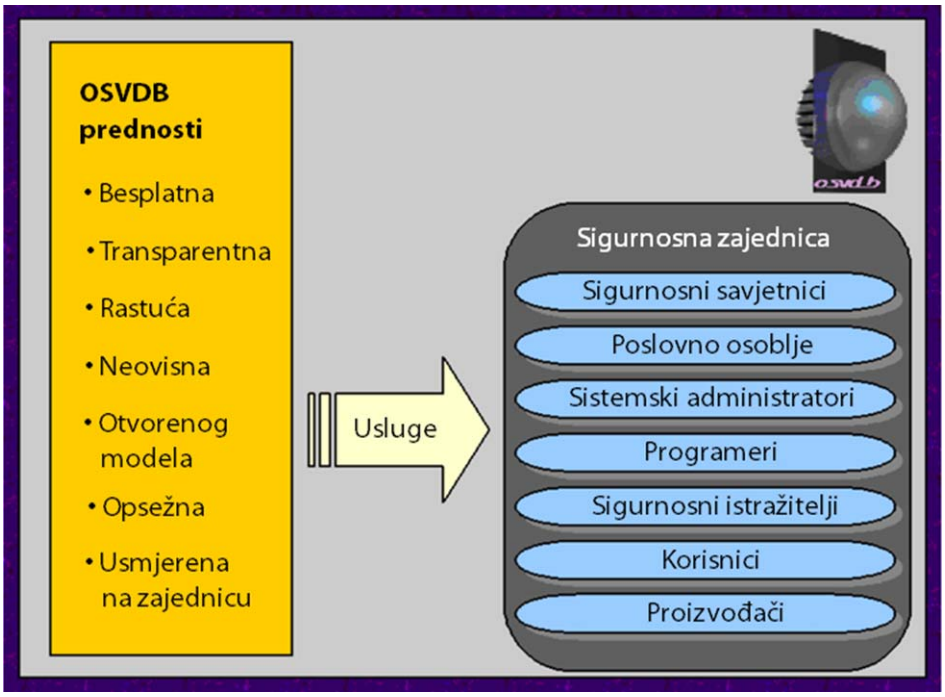
4.2. OSVDB

OSVDB baza podataka uključuje veliku kolekciju sigurnosnih ranjivosti koje su besplatno dostupne informatičko-sigurnosnoj zajednici. Sadrži informacije o poznatim sigurnosnim ranjivostima u operacijskim sustavima, programskim proizvodima, protokolima, sklopovskim uređajima i drugim elementima računalnih sustava i mreža. Namjena joj je biti centralna baza ranjivosti na Internetu.

Koriste ju mnogi korisnici poput:

- poduzeća koja trebaju znati koji je element njihovog trenutnog ili planiranog okruženja ranjiv na neki napad,
- sistemski administratori koji žele biti obaviješteni o trenutnim sigurnosnim nedostacima i načinima njihova otklanjanja,
- osobe koje razvijaju programske proizvode kako ne bi iste pogreške uključili u trenutne i buduće projekte i
- osobe koje se bave sigurnošću kako bi mogli osigurati svoje proizvode ili usluge.

Slika 8 prikazuje prednosti i korisnike OSVDB baze.



Slika 8. Prednosti i korisnici OSVDB baze
Izvor: OSVDB

Trenutno djeluje kao aktivna web aplikacija i ima dva osnovna dijela:

1. prezentacijski dio – moguće ga je pretraživati i dojavljivati nove ranjivosti,
2. administracijski dio – omogućuje dodavanje ili izmjenu ranjivosti.

U procesu održavanja baze sudjeluju brojni pojedinci podijeljeni u sljedeće uloge:

- **moderatori** – zaduženi za većinu poslova uključujući upravljanje sadržajem, pregled i odobravanje novih unosa u bazu i sl. Moderatori imaju zadatak provjeriti da li prijavljene ranjivosti već postoje u bazi te odlučiti o dodavanju novih.
- **korisnici** – osim same uporabe baze, svaki korisnik može predložiti osvježavanje podataka o ranjivostima.
- **upravitelji podacima** (eng. *datamanglers*) – korisnici koji su odgovorni za osvježavanje unosa o ranjivostima kako bi se osigurala pouzdanost i dostupnost informacija.
- **programeri** - grupa koja je zadužena za pravilan rad baze i sve ostale tehničke aspekte.

Postupak upisa novih ranjivosti započinje kada moderatori identificiraju nove ranjivosti i dodijele im određenog upravitelja podacima (eng. *datamangler*). On pretražuje Internet kako bi pronašao informacije koje opisuju ranjivost. Moderator pregledava informacije te objavljuje prikupljene podatke. Ovakav postupak se ponavlja što omogućuje brz i jednostavan pristup novim ranjivostima. Prema tome, baza podataka može se proširiti na dva načina, u slučaju da se prikupe novi podaci o nekoj ranjivosti ili kada se unose nove ranjivosti.

4.3. Secunia

Secunia je organizacija koja se bavi identificiranjem i uklanjanjem prijetnji raznih ranjivosti njihovim praćenjem te pružanjem podataka korisnicima i zajednici. Surađuje s brojnim proizvođačima, istraživateljima, sigurnosnim stručnjacima, kupcima, sigurnosnim organizacijama te korisnicima.

Secunia održava bazu podataka sa svim preporukama i otkrivenim ranjivostima, a sadrži informacije bez obzira na tip programa ili operacijskog sustava. Radi se o javnoj bazi podataka s informacijama namijenjenim istraživateljima, proizvođačima i korisnicima. Može se iskoristiti prilikom provjere određenog proizvoda ili poduzimanja akcija osiguravanja sustava od poznatih ranjivosti.

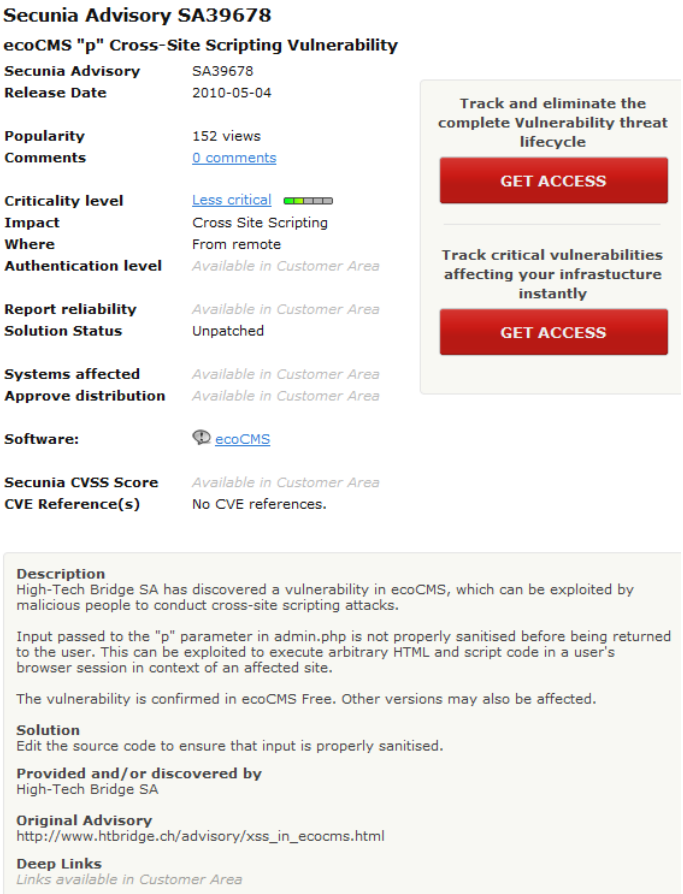
Baza sadrži više tisuća zapisa o ranjivostima, a svakog dana upisuje se u prosjeku 20 novih. Svaka osoba može u bilo kojem trenutku prijaviti novu ranjivost preko web stranice organizacije. Dojave o

ranjivostima smatraju se javnim informacijama te se objavljuju u obliku preporuke (osim ako proizvođač nije zatražio pomoć oko otklanjanja nedostatka).

Prilikom dojave sigurnosne ranjivosti potrebno je osigurati postojanje sljedećih podataka:

- ugroženi operacijski sustav/program (uključujući potpune podatke o inačici),
- način iskorištavanja ranjivosti,
- rezultat uspješnog iskorištavanja ranjivosti i
- dodatni podaci koji će olakšati postupak verifikacije.

Svaka prijavljena ranjivost se istražuje te prihvaća ili odbacuje. Ukoliko se ranjivost prihvati podaci o njoj dodaju se u bazu podataka u obliku preporuke. Tada je moguće vrlo jednostavno pretraživanje baze podataka preko identifikatora. Primjer jednog zapisa o ranjivosti u obliku preporuke dan je na Slika 9.



Slika 9. Primjer Secunia preporuke
Izvor: Secunia

4.4. SecurityFocus

Od samog osnivanja, SecurityFocus bio je glavna potpora sigurnosnoj zajednici svakodnevno donoseći novosti i detaljne dokumente iz područja sigurnosti. Usmjeren je na ključna područja koja su od velikog značenja za sigurnosnu zajednicu.

Jedan od najznačajnijih projekata je *mailing* lista za raspravu i objavu sigurnosnih ranjivosti pod nazivom Bugtraq. Na listi sudjeluju članovi iz cijelog svijeta te vode rasprave o svim aspektima sigurnosnih ranjivosti. Trenutno postoji 31 *mailing* lista koje moderatori održavaju odbacivanjem sve neželjene pošte. Također, baza podataka s ranjivostima pruža sigurnosnim profesionalcima najnovije informacije o ranjivostima na svim platformama i uslugama.

Glavna obilježja web stranice SecurityFocus su:

- pruža mjesto za dijeljenje informacija,
- omogućuje rasprave o novim idejama,
- omogućuje dijeljenje novih tehnologija,
- povezuje sigurnosnu zajednicu,
- besplatna je.

Početkom godine, objavljeno je kako se sav sadržaj organizacije SecurityFocus od 15. ožujka 2010. prenosi u organizaciju Symantec. Ipak, sve *mailing* liste (uključujući Bugtraq), kao i baza podataka, ostat će dostupne na web stranicama organizacije SecurityFocus. Neće biti nikakvih promjena u listama ili politikama, niti u timu zaduženom za održavanje istih. Nastavit će se s održavanjem baze podataka kako bi uvijek sadržavala najnovije i pouzdane informacije.

4.5. CERT

1988. godine osnovan je centar CERT/CC (eng. *CERT Coordination Center*) kao odgovor na ugrožavanje brojnih računala Morrisovim crvom. Centar ima zadatak analiziranja ranjivosti te odgovaranja na velike sigurnosne incidente. Tokom godina rastao je broj ranjivosti i napada te njihova složenost što je dovelo do pripajanja centra programu CERT. Spomenuti program je dio SEI (eng. *Software Engineering Institute*) instituta, vladinog istraživačkog i razvojnog centra. Usmjeren je na razvoj i promoviranje uporabe tehnologija i praksi za upravljanje sustavima kako bi bili otporni na napade, ograničili štetu ili osigurali kontinuirani rad kritičnih usluga.

Područja rada programa CERT:

- osiguravanje programa – analiza stanja sigurnosti na Internetu i prijenos informacija sigurnosnoj zajednici. CERT/CC upravlja javnim izvorima informacija o ranjivostima te prima izvješća. Nakon analize potencijalnih ranjivosti, stručnjaci obavještavaju proizvođače te sudjeluju u ispravljanju nedostataka.
- osiguravanje sustava – analiziranje otpornosti sustava na napade te pronalaženje načina poboljšanja sigurnosti. Također, uključuje i razvoj tehnika za predviđanje potencijalnih prijetnji na Internetu.
- sigurnost organizacija – pomoć organizacijama u zaštiti i obrani.
- koordinirani odgovori – globalna podrška za adresiranje sigurnosnih problema koja pomaže u formiranju timova za oporavak od incidenata.
- edukacija i treniranje – javni tečajevi za tehničko osoblje, administratore te druge korisnike.

CERT CC se bavi analizom rizika u programima i sustavima s fokusom na identifikaciju potencijalnih i postojećih ranjivosti, obavještavanje administratora te suradnju s proizvođačima kako bi se otklonio problem. Analiza ranjivosti je jedno od vrlo važnih područja rada čiji je cilj otkriti ranjivosti u gotovim proizvodima, kao i u onima u razvoju. Otkrivanje ranjivosti podijeljeno je u tri faze:

1. pronalaženje ranjivosti (eng. *vulnerability discovery*) – pružanje pomoći u obliku znanja, tehnologija i alata kako bi se otkrile ranjivosti u proizvodima.
2. sanacija ranjivosti (eng. v*ulnerability remediation*) – pristup uklanjanju ranjivosti koji uključuje najbolje prakse, izmjenu konfiguracije ili arhitekture i primjenu rješenja. Sastoji se od četiri koraka:
    - prikupljanje (eng. *collection*) – prikupljanje ranjivosti obavlja se praćenjem javnih izvora ranjivosti i obradom primljenih izvješća (izbacuju se lažne dojave i duplikati).
    - analiza (eng. *analysis*) – nakon prikupljanja, određuje se ozbiljnost ranjivosti, ugroženi sustavi, način iskorištavanja te posljedice uspješnog iskorištavanja. Uključuje ispitivanje, analizu te suradnju i konzultiranje s proizvođačima i drugim stručnjacima.
    - koordinacija (eng. *coordination*) – ako se radi o izravnoj prijavi ranjivosti, pokreće se suradnja s proizvođačima prije bilo kakve javne objave ranjivosti.
    - Objava (eng. *disclosure*) – nakon koordinacije s proizvođačem, potrebno je obavijestiti javnost o otkrivenoj ranjivosti.

3. blog za analizu ranjivosti (eng. *vulnerability analysis blog*) – uključuje tekstove iz područja sigurnosti.

Svaka otkrivena i analizirana ranjivost ostaje zapisana u bazi podataka. Statistički podaci pokazuju da je broj ranjivosti koje se objave tokom jedne godine znatno porastao u usporedbi s prvim godinama rada CERT-a. Slika 10 prikazuje broj objavljenih sigurnosnih ranjivosti kao i upozorenja kroz gotovo 10 godina rada. Prvi stupac sadrži informacije o objavljenim ranjivostima, tj. tehničke podatke i rješenja. Tehnička sigurnosna upozorenja u drugom stupcu odnose se na dokumente koji donose informacije o trenutnim sigurnosnim problemima, ranjivostima i načinima iskorištavanja. Posljednji stupac sadrži broj objavljenih sigurnosnih upozorenja, tj. dokumenata o koracima zaštite koje korisnici i organizacije mogu poduzeti.

Razdoblje:	Objavljene ranjivosti:	Objavljena tehnička upozorenja:	Objavljena upozorenja:
Q1-Q3, 2008	*145*	*29*	*22*
2007	*366*	*42*	*31*
2006	*422*	*39*	*37*
2005	*285*	*22*	*11*
2004	*341*	*27*	*17*
2003	255	-	-
2002	375	-	-
2001	326	-	-
2000	47	-	-
1999	3	-	-
1998	8	-	-
Ukupno:	**2,573**	**159**	**118**

Slika 10. Broj prijavljenih ranjivosti u CERT bazu
Izvor: CERT

Potrebno je naglasiti da od 2004. godine CERT usko surađuje s organizacijom US-CERT te objavljuje upozorenja u njihovo ime.

4.5.1. US-CERT

Organizacija US-CERT usko surađuje s centrom CERT/CC s ciljem umanjivanja posljedica napada računalnih kriminalaca. Osnovana je kako bi iskoristiti kapacitete centra CERT/CC u svrhu zaštite sustava i odgovaranja na napade. Osim toga, ona osigurava poveznicu centra CERT/CC s Ministarstvom domovinske sigurnosti, surađuje s vladinim agencijama, industrijskim i istraživačkim te drugim organizacijama kako bi pružila javnosti informacije o računalnim prijetnjama. Sve informacije su dostupne na web stranici, *mailing* listi i RSS kanalima organizacije.

US-CERT pruža informacije o sigurnosti od računalnih napada, uključujući upozorenja o kritičnim sigurnosnim problemima za korisnike. Najveća razlika u odnosu na CERT/CC preporuke je u povećanom broju informacija za nestručne korisnike. US-CERT, osim informacija iz centra CERT/CC, uključuje razne podatke prikupljene od drugih organizacija. Organizacija US-CERT održava bazu podataka o svim objavljenim ranjivostima.

4.6. Ostale baze

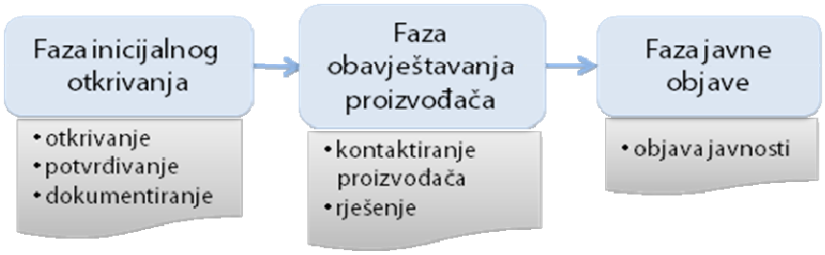
Organizacija CIAC (eng. *Computer Incident Advisory Capability*) je osnovana kao tim za rješavanje incidenata, a temeljni cilj joj je bio podići svijest o opasnostima s Interneta. Usmjeravali su se većinom na sigurnosne ranjivosti, viruse i druge sigurnosne probleme. Objavljivali su izvješća i preporuke sve dok nisu preimenovani u DOE-CIRC te postali dio Ministarstva Energije SAD-a.

ISS (eng. *Internet Security Systems'*) X-Force je organizacija koja pruža najnovije informacije o internetskim prijetnjama i ranjivostima kroz upozorenja i preporuke. Svako upozorenje uključuje i informacije o načinu zaštite od prijetnji putem IBM ISS proizvoda. Objavljuju informacije o kritičnim ranjivostima koje su otkrili te o novim zlonamjernim programima.

Proces otkrivanja ranjivosti sastoji se od sljedećih faza:

1. Faza inicijalnog otkrivanja (eng. *initial discovery phase*) – tim otkriva i potvrđuje ranjivost te ju dokumentira u nacrtu preporuke.
2. Faza obavještavanja proizvođača (eng. *vendor notification phase*) – tim uspostavlja inicijalnu komunikaciju s proizvođačem kako bi ga obavijestili o pronađenoj ranjivosti. Zatim proizvođaču šalju nacrt preporuke te surađuju s njim kako bi razvio rješenje. Sljedeći korak je rezervacija CVE broja te stvaranje potpune preporuke. X-Force tim tada smije objaviti preporuku.
3. Faza javne objave (eng. *public disclosure phase*) – tim koordinira javnom objavom preporuke.

Opisane faze prikazane su na Slika 11.



Slika 11. Faze otkrivanja ranjivosti ISS X-Force tima

Security Tracker je usluga koja pomaže u praćenju posljednjih sigurnosnih ranjivosti preko upravljanja s izvješćima iz raznih izvora. U svojim upozorenjima uključuje CVE identifikatore te omogućuju pretragu na temelju istih. Namijenjena je za profesionalce u području informacijskih tehnologija poput administratora sustava, konzultanata, upravitelja, programera i sl.

Dobre osobine usluge su:

- brže pronalaženje obavijesti o sigurnosnim nedostacima,
- bolje praćenje izdavanja nadogradnji za sigurnosne proizvode,
- omogućuje primanje obavijesti samo o određenim proizvodima.

5. Standardiziranje ranjivosti i proizvoda

5.1. CVE

CVE standard donosi jedinstveno označavanje ranjivosti s ciljem rješavanja sljedećih problema:

- Nekonzistentno pretvaranje nazivlja (eng. *inconsistent naming conventions*) – razne baze podataka nazivaju istu ranjivost na više načina što otežava pretraživanje i povezivanje informacija o istoj ranjivosti iz različitih izora. Kako bi se to otklonilo uveden je referentni sustav označavanja na koji se moguće pozvati u svakom sigurnom upozorenju ili izvješću.
- Različite perspektive iste ranjivosti detektirane različitim alatima (eng. *different perspectives of the same vulnerability detected by different tools*) – različiti alati generiraju različita izvješća o ranjivostima. Na primjer, skeneri virusa pretražuju uzorke napada, a alati za procjenu ranjivosti instalirane aplikacije. Kao rezultat analize potrebno je imati rezultate koji se mogu usporediti, poput referentnog broja za istu ranjivost.
- Besplatna i potpuna distribucija (eng. *free and completed distribution*) – razni izvori informacija zaštićeni su autorskim pravima ili nisu potpuni. Uvođenje standarda omogućuje javno objavljivanje svih informacija o ranjivostima u obliku besplatnom za distribuciju.

CVE je danas standard koji koriste mnogi proizvođači sigurnosnih proizvoda, a brojne organizacije sudjeluju u njegovom razvoju. Uveden je jedinstveni proces praćenja ranjivosti i njihova označavanja.

5.1.1. CVE kompatibilnost

CVE kompatibilnost označava da alat, web stranica, baza podataka ili drugi sigurnosni proizvod/usluga koriste CVE identifikatore kako bi se povezali s drugim proizvodima.

Omogućava sljedeće radnje:

- pretraživanje po CVE identifikatorima kako bi se pronašle povezane informacije,
- predstavljanje informacija uz uključivanje sličnih CVE identifikatora,
- označavanje prema inačici CVE.

Različiti alati pružaju drugačiji oblik konvergencije ili povezivanja kroz CVE identifikatore.

Svaki kompatibilni alat, usluga ili proizvod dobije oznaku CVE kompatibilnosti prikazanu na Slika 12. Trenutno postoji 95 proizvoda i usluga te 52 organizacije koje sadrže spomenutu oznaku.

Slika 12. Logo CVE kompatibilnosti
Izvor: CVE

Kako bi se postao član grupe kompatibilnih proizvoda potrebno je primijeniti proces prilagodbe i kompatibilnosti (eng. *Adoption and Compatibility Process*) te primijeniti brojne zahtjeve i preporuke (eng. *Requirements and Recommendations for CVE Compatibility*). Spomenuti proces sastoji se od više koraka, a započinje kada organizacije postanu svjesne vrijednosti i potencijala CVE standarda.

5.2. CWE

CWE (eng. *Common Weakness Enumeration*) standard je internacionalni, besplatni i javni standard koji pruža jedinstvenu skupinu sigurnosnih ranjivosti programa omogućujući efektivnije rasprave, opise te odabir sigurnosnih alata koji mogu detektirati neku ranjivost. Također usmjeren je na bolje razumijevanje i upravljanje sigurnosnim ranjivostima vezanim uz arhitekturu i dizajn.

Osnovna zadaća inicijative je osnažiti postojeće procese praćenja ranjivosti u zajednici, što se posebno odnosi na brojne ranjivosti koje se nalaze na CVE listi. Teži se razvoju specifične definicije elemenata kako bi se klasificirali u strukturu sličnu stablu (Slika 13). Dodatno, definirano je odgovarajuće označavanje

između CWE i CVE imena kako bi svaka CWE grupa imala listu posebnih CVE identifikatora koji pripadaju toj kategoriji sigurnosnih ranjivosti. U konstrukciji CWE liste i stabla klasifikacije teži se maksimalnoj konvergenciji preko konceptualnih, poslovnih i tehničkih domena.

Značajke CWE standarda:

- Pružanje osnovnog jezika za raspravu, pronalaženje i rukovanje s uzrocima sigurnosnih ranjivosti prilikom njihove pojave u kodu, dizajnu ili arhitekturi.
- Omogućuje proizvođačima sigurnosnih alata i pružateljima sigurnosnih usluga informiranje o postojećim ranjivostima koji se odnose na njihov rad i korisnike. Također, konvergencijom sa standardom postiže se kompatibilnost te ostvaruje pravo objave oznake „*CWE Compatibility*".
- Omogućuje usporedbu, provjeru i odabir sigurnosnih alata i usluga koji su najprikladniji za potrebe korisnika. Također, moguće je provjeriti konvergenciju alata i usluga s CWE standardom.
- Omogućuje vladi i organizacijama uporabu standardizacije u ugovorima.

- Coding Standards Violation - *(710)*
  - Embedded Malicious Code - *(506)*
    - Logic/Time Bomb - *(511)*
    - Spyware - *(512)*
    - Trapdoor - *(510)*
    - Trojan Horse - *(507)*
      - Non-Replicating Malicious Code - *(508)*
      - Replicating Malicious Code (Virus or Worm) - *(509)*
  - Failure to Fulfill API Contract ('API Abuse') - *(227)*
    - Explicit Call to Finalize() - *(586)*
    - Failure to Follow Specification - *(573)*
      - Duplicate Operations on Resource - *(675)*
        - Double Decoding of the Same Data - *(174)*
        - Multiple Binds to the Same Port - *(605)*
        - *Double Free - (415)*
        - *Multiple Locks of a Critical Resource - (764)*
        - *Multiple Unlocks of a Critical Resource - (765)*
      - EJB Bad Practices: Use of Class Loader - *(578)*
      - EJB Bad Practices: Use of Sockets - *(577)*
      - Function Call with Incorrectly Specified Arguments - *(628)*
        - Function Call With Incorrect Argument Type - *(686)*
        - Function Call With Incorrect Number of Arguments - *(685)*
        - Function Call With Incorrect Order of Arguments - *(683)*
        - Function Call With Incorrect Variable or Reference as Argument - *(688)*
        - Function Call With Incorrectly Specified Argument Value - *(687)*
          - Use of umask() with chmod-style Argument - *(560)*
      - Improper Following of Chain of Trust for Certificate Validation - *(296)*
      - Improperly Implemented Security Check for Standard - *(358)*
      - Incorrect Check of Function Return Value - *(253)*
      - J2EE Bad Practices: Non-serializable Object Stored in Session - *(579)*
      - Missing Critical Step in Authentication - *(304)*

Slika 13. CWE stablo
Izvor: CWE

5.2.1. CWE lista

U definiranju organizacijskih struktura za CWE elemente, želi se postići jednostavnost opisa prilagođena raznolikim korisnicima koja je prikladna za brojne namjene kroz uporabu slojeva. Trenutno se koristi tzv. *three-tiered* pristup koji sadrži sljedeće slojeve:

- najniža razina - sadrži potpunu CWE listu (tisuću čvorova) primarno namijenjenu proizvođačima alata i istražiteljima,
- srednja razina – sadrži grupirane srodne CWE grupe (25-50 čvorova) namijenjene osobama koje razvijaju programske proizvode,
- gornja razina – sadrži grupirane čvorove sa srednje razine, a namijenjena je definiranju strateških klasa ranjivosti za korisnike, istražitelje, proizvođače i druge.

Prema tome, CWE standard sadrži brojne čvorove, a neki od značajnijih su:

- *„80 - Basic XSS“* – koristi se niz podataka i naredbi uz uporabu posebnih elemenata, a napadač uvodi takve podatke u HTML niz kako bi doveo do pokretanja XSS (eng. *Cross-site scripting*) napada.
- *„89 – SQL Injection“* – uključuje miješanje podataka i naredbi u jednom nizu uz uporabu posebnih elemenata za njihovo razdvajanje. Pogreška se pojavljuje kada podaci sadrže posebne elemente koji uzrokuju krivu interpretaciju nizova. Tada napadač može podmetnuti podatke kojima će narušiti sigurnost te ostvariti povećanje prava na sustavu ili sl.
- *„190 - Integer Overflow“* – koristi se broj kako bi se kontroliralo ili utjecalo na resurs. Napadač može generirati taj broj uz određenu manipulaciju (npr. veće vrijednosti nego je dozvoljeno) te uzrokovati cjelobrojno prepisivanje.
- „401 - Memory leak“ – koristi se dinamičko alociranje memorije u jednoj instanci programa, a napadač navodi program na prestanak rada bez oslobađanja zauzete memorije.
- *„121 - Stack Overflow“* – program prima ulazne vrijednosti u spremnik te provodi daljnju obradu i sprema rezultat u spremnik. Napadač navodi sustav na stvaranje rezultata koji je veći od veličine spremnika te uzrokuje prepisivanje spremnika.

5.3. CPE

CPE (eng. *Common platform enumeration*) je strukturirana shema za imenovanje informatičko tehničkih sustava, platformi i programskih paketa. Temeljena je na generičkoj sintaksi za URI (eng. *Uniform Resource Identifiers*) nizove. Uključuje formalni oblik imena, jezik za opis složenih platformi, metodu za provjeru imena na sustavu te opisni format za povezivanje teksta i imena. Pruža sustav za jedinstveno označavanje IT platformi na kojima su pronađene sigurnosne ranjivosti. Uspjeh CPE strukture ovisi o sudjelovanju sigurnosne zajednice, a svaki korisnik se može uključiti u razvoj i rasprave.

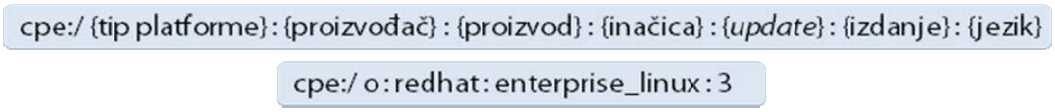
CPE specifikacija uključuje:

1. sintaksu za imenovanje tj. konstruiranje CPE imena za proizvode,
2. algoritam za provjeru podudarnosti,
3. jezik za opis složenih platformi i
4. XML shemu za povezivanje opisa i informacija s imenom.

Preko navedenih značajki kreira se rječnik s CPE imenima koji su predstavljeni URI nizovima. Svako ime sadrži prefiks „cpe“ kojeg slijedi sedam različitih komponenti:

- tip platforme – svakoj platformi može se dodijeliti jedna od tri oznake:
  - h – sklopovlje (eng. *hardware*),
  - o – operacijski sustav (eng. *operating system*),
  - a – aplikacija (eng. *application*).
- proizvođač – organizacija koja proizvodi platformu.
- proizvod – ime proizvoda,
- inačica – inačica proizvoda,
- *update* – informacije o nadogradnji,
- izdanje – ako je definirano za platformu,
- jezik – jezik povezan s platformom.

Prve dvije komponente su obavezne, a ostale su opcionalne. Navedene komponente pomažu izgraditi konzistentno i jedinstveno ime. Struktura i primjer CPE imena dani su na Slika 14.



Slika 14. Struktura i primjer CPE imena
Izvor: CWE

Individualna CPE imena olakšavaju adresiranje jednog određenog dijela sustava. Za identificiranje kompleksnijih tipova platformi potrebno je uvesti način kombiniranja različitih CPE imena preko logičkih operatora. Ovakav se pristup koristi kada korisnik ima potrebu identificirati platformu s određenim operacijskim sustavom i aplikacijom. U tu svrhu koristi se CPE jezik koji omogućuje kombiniranje imena s operacijskim sustavima, aplikacijama i dr.

Provjera podudaranja koristi se u procesu određivanja da li dano CPE ime ili izraz u CPE jeziku specificira platformu koja je definirana grupom poznatih CPE imena. Na primjer, pri ispitivanju nekog sustava s alatima za analizu potrebno je moći odrediti da li neko CPE ime odgovara sustavu.

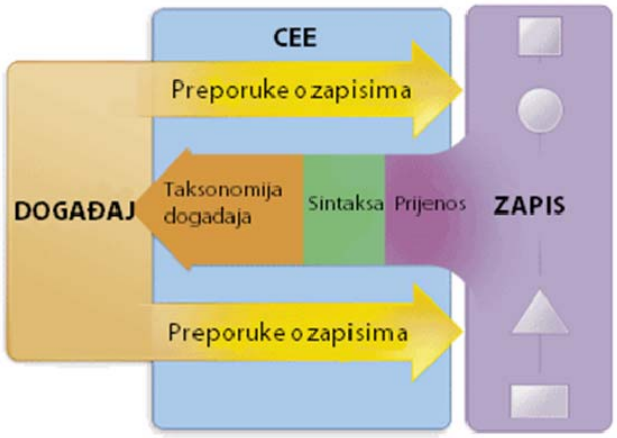
5.4. Ostali standardi

CCE (eng. *Common Configuration Enumeration*) pruža jedinstvene identifikatore za probleme u konfiguraciji sustava, kako bi se osiguralo brzo povezivanje konfiguracijskih podataka preko različitih izvora podataka i alata. Sadrži listu jedinstvenih identifikatora za određivanje problema u konfiguraciji kako bi se poboljšao rad. Predstavlja most između prirodnog jezika, dokumenata o uputama za konfiguraciju te konfiguracijskih alata. Svaki element u CCE listi sadrži:

- CCE identifikator – jedinstvena oznaka, npr. CCE-2715-1;
- opis – kratki opis konfiguracijskog problema;
- konceptualne parametre (eng. *Conceptual Parameters*) – parametri koje je potrebno specificirati kako bi se implementirao CCE u sustav;
- povezani tehnički mehanizmi (eng. *Associated Technical Mechanisms*) – jedan ili više načina za postizanje željenih rezultata;
- reference – poveznice na dodatnu dokumentaciju.

CEE (eng. *Common Event Expression*) standardizira način na koji se opisuju, zapisuju i razmjenjuju događaji na računalu. Namijenjen je postizanju učinkovitijih i boljih rezultata u povezivanju, upravljanju i rukovanju zapisima. Osnovne komponente, prikazane na Slika 15, su:

1. Taksonomija događaja (eng. *Event Taxonomy*) – specificira tip događaja koji može biti prijava korisnika, povezivanje na Internet, povećanje ovlasti i dr. Omogućuje zapis svih događaja koji pripadaju jednom tipu na jednak način.
2. Sintaksa zapisa (eng. *Log Syntax*) – definira način zapisa događaja i njegovih detalja, a može biti u XML, tekstualnom obliku ili binarno kodiran. Kako bi se održala konzistentnost, CEE pruža rječnik podataka tj. skupinu atributa koji se mogu koristiti za detaljniji opis događaja.
3. Prijenos zapisa (eng. *Log transport*) – potreban je za razmjenu zapisa, a definira se poseban način prijenosa.
4. Preporuke o spremanju zapisa (eng. *Logging Recommendations*) – skupina najboljih praksi za spremanje zapisa.

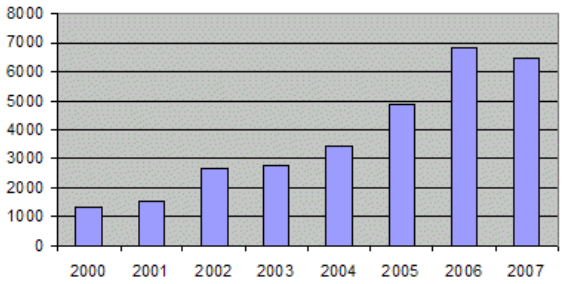


Slika 15. Komponente CEE
Izvor: CEE

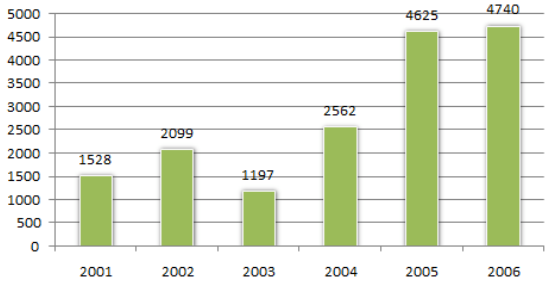
6. Problemi

6.1. Pouzdanost informacija

Svakodnevno se otkiva sve veći broj novih sigurnosnih ranjivosti u raznim proizvodima i sustavima. Statistički podaci o unesenim ranjivostima u razne baze podataka pokazuju stalan porast . Na Slika 16 prikazan je porast broja ranjivosti u CVE bazi u razdoblju od 2000. do 2007. godine, a na Slika 17 promjena ranjivosti u ISS X-Force bazi od 2001. do 2006. godine. Navedeni podaci svjedoče o stalnom pronalaženju novih ranjivosti.



Slika 16. Ranjivosti u CVE bazi
Izvor: CVE



Slika 17. Ranjivosti u ISS X-Force bazi
Izvor: ISS

Kako bi se mogla pravilno pratiti i objaviti javnosti, svaka novootkrivena ranjivost mora biti detaljno analizirana kako bi se provjerila točnost informacija koje su prijavljene sigurnosnoj organizaciji. Sigurnosne organizacije dužne su provjeriti informacije i osigurati njihovu ispravnost. Iako su suočene s velikom količinom podataka koju moraju obraditi brzo i pouzdano, organizacije si ne mogu priuštiti pogrešne procjene i objavu netočnih upozorenja.

6.2. Javno objavljivanje ranjivosti

Većina opisanih baza podataka i organizacija za praćenje ranjivosti pruža neograničen pristup informacijama za sve korisnike, proizvođače i istražitelje. Često se javlja zabrinutost radi javne objave ranjivosti, načina njezine zlouporabe te popisa ugroženih sustava i proizvoda. Takve ranjivosti mogu nositi ozbiljne posljedice poput mogućnosti stjecanja administratorskih ovlasti na sustavu ili pokretanja nekog od napada koji će ugroziti pravilan rad sustava (npr. napad uskraćivanja usluga).

Objavljene informacije mogu pomoći napadačima u traženju ranjivih sustava te iskorištavanju ranjivosti. Također, mogu biti iskorištene u svrhu stvaranja zlonamjernih alata ili programa za napade na korisnička računala.

Ipak, javnim objavljivanjem ranjivosti korisnike ugroženih proizvoda upozorava se na postojanje sigurnosnih problema te navodi na traženje rješenja. Oni tada mogu potražiti način otklanjanja ranjivosti te spriječiti njezinu zlouporabu. Ukoliko je proizvođač razvio odgovarajuću sigurnosnu nadogradnju, korisnici dobivaju informacije o načinu njezina preuzimanja i primjene. U suprotnom, korisnicima se daju detaljne upute o nekom načinu na koji mogu privremeno smanjiti rizike od postojećih ranjivosti.

6.3. Zero-day ranjivosti

Zero-day ranjivosti su one ranjivosti u programima koje nisu poznate njihovim proizvođačima. Za njih ne postoji programska nadogradnja koja rješava problem. Predstavljaju vrlo opasnu prijetnju jer se korisnici ne mogu zaštititi od takvih napada. Više podataka o ovom obliku ranjivosti moguće je pronaći u CERT dokumentu „Zero day ranjivosti“:

http://www.cert.hr/documents.php?id=405

Otkrivanje ovakvih ranjivosti predstavlja vrlo osjetljivu temu u sigurnosnoj zajednici. Brojne sigurnosne organizacije pridržavaju se pravila o potpunom razotkrivanju podataka o ranjivostima (eng. *full disclosure*). To bi značilo da podržavaju javno otkrivanje svih detalja o sigurnosnom problemu pa čak i metoda zlouporabe. Iza ovakvog koncepta stoji vjerovanje kako će proizvođačima biti u interesu otkloniti ranjivosti koje su u potpunosti javno otkrivene. Osnovna prednost potpune objave svih podataka o ranjivosti je brže prikupljanje podataka i objava potrebnih programskih ispravka.

Ipak, dio sigurnosne zajednice protivi se takvoj praksi navodeći kako ranjivost za koju ne postoji nadogradnja treba prvo prijaviti proizvođaču i sigurnosnim organizacijama. Time se proizvođaču daje mogućnost da ukloni ranjivost te izda sigurnosno upozorenje.

Prema tome, uvodi se nova politika oko objave informacija o *zero-day* ranjivostima, koja uključuje obavještavanje proizvođača te dogovor roka za izdavanje nadogradnje te datuma obavještavanja javnosti.

7. Budućnost

Prema svim dostupnim podacima iz raznih izvora informacija o sigurnosnim ranjivostima, može se uvidjeti stalno povećavanje njihova broja. Svakodnevno se otkrivaju nove, ali i nadopunjuju informacije o prethodno otkrivenim ranjivostima. Takav tempo rasta broja ranjivosti dovodi do brzog širenja baza, ali i do potrebe za razvojem sistematičnog sustava njihova praćenja i analiziranja. Sigurnosne organizacije uvode vlastite postupke praćenja ranjivosti stvarajući nove baze, identifikatore i standarde.

Prema tome, u budućnosti se može očekivati razvoj novih baza i standarda za otkrivanje ranjivosti, njihovu analizu, praćenje te objavu. Oni će za cilj imati bolju povezanost informacija iz raznih izvora podataka te omogućavati bržu i jednostavniju pretragu. Težit će se boljoj konzistentnosti te konvergenciji, ne samo baza i standarda, nego i alata za analiziranje ranjivosti. Usporedno razvoju novih baza, očekuje se usavršavanje postojećih dodavanjem novih specifikacija i uvođenjem sustavnih tehnika za njihovo rukovanje.

Također, u budućnosti se očekuje podizanje svijesti korisnika o prijetnjama koje nose sigurnosne ranjivosti te mogućnostima koje nudi njihova javna objava. Takav scenarij potaknuo bi bolju uključenost korisnika u projekte praćenja ranjivosti te smanjio broj iskorištenih propusta za koje postoji odgovarajuća nadogradnja.

Osim suradnje s korisnicima, predviđa se uključivanje cjelokupne sigurnosne zajednice (raznih organizacija, istražitelja, proizvođača i sl.) u postupak otkrivanja, ispravljanja i objave ranjivosti. Posebno se očekuje poboljšanje komunikacije s proizvođačima kako bi se pronađene ranjivosti što prije i na adekvatan način ispravile.

8. Zaključak

Napredak tehnologije i računarstava, kao i širenje internetskih usluga, dovodi do pojačane potrebe za raznovrsnim programskim alatima, uslugama i sustavima. Ubrzan razvoj takvih proizvoda često dovodi do raznih pogrešaka u implementaciji i kodu i. što otvara mogućnosti za pojavu sigurnosnih ranjivosti. Kako bi se izbjegli veliki rasponi štete koju bi moglo imati iskorištavanje neispravljenih ranjivosti u popularnim i široko korištenim proizvodima, razvijen je postupak za njihovo praćenje. On uključuje otkrivanje i analizu ranjivosti, njihovu prijavu proizvođaču, suradnju s proizvođačem kako bi se ranjivost uklonila te javnu objavu svih informacija. Takva praksa pokazala se uspješnom u suzbijanju broja uspješno iskorištenih sigurnosnih ranjivosti, kao i u navođenju proizvođača na poboljšanje vlastitih proizvoda. Razlog tome je što postojanje baza podataka s ranjivostima omogućuje korisnicima lakše pretraživanje i provjeravanje korištenih programa i sustava. U budućem razvoju, moguće je očekivati napredak standarda za označavanje ranjivosti te bolju konvergenciju između raznih izvora podataka, alata, sigurnosnih organizacija, proizvođača i korisnika.

9. Reference

[1] Organization for Internet Safety: „Guidelines for Security Vulnerability Reporting and Response“, http://www.oisafety.org, 2004.

[2] Sigurnosna ranjivost, http://en.wikipedia.org/wiki/Security_vulnerability, svibanj, 2010.

[3] CVE, http://cve.mitre.org/index.html, svibanj, 2010.

[4] SANS Institute, InfoSec Reading Room: „Vulnerability naming schemes and description languages: CVE, Bugtraq, AVDL and VulnXML“, http://www.sans.org/reading_room/whitepapers/threats/vulnerability-naming-schemes-description-languages-cve-bugtraq-avdl-vulnxml_1058, travanj, 2003.

[5] OSVDB, http://osvdb.org/, svibanj, 2010.

[6] Mitre, http://www.mitre.org/, svibanj, 2010.

[7] Secunia, http://secunia.com/, svibanj, 2010.

[8] SeucurityFocus, http://www.securityfocus.com/, svibanj, 2010.

[9] CERT, http://www.cert.org/, svibanj, 2010.

[10] US-CERT, http://www.us-cert.gov/index.html, svibanj, 2010.

[11] CWE, http://cwe.mitre.org/, svibanj, 2010.

[12] CPE, http://cpe.mitre.org/, svibanj, 2010.

[13] CCE, http://cce.mitre.org/, svibanj, 2010.

[14] CIAC, http://en.wikipedia.org/wiki/Computer_Incident_Advisory_Capability, svibanj, 2010.

[15] ISS X-Force, http://xforce.iss.net/, svibanj, 2010.

[16] Security Tracker, http://www.securitytracker.com/startup/index.html, svibanj, 2010.