CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

CVSS - Common Vulnerability Scoring System

NCERT-PUBDOC-2010-01-288

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

Informacije su danas najvrjednija imovina svakog poslovnog sustava, tj. predstavljaju njegov intelektualni kapital. One se nalaze u mnogim oblicima i na različitim medijima, a brzi razvoj primjene informacijsko-komunikacijske tehnologije uzrokuje i sve veće mogućnosti napada na informacijske sustave i zlouporabu informacija. Razvojem visokih tehnologija modernog doba, većina se organizacija u velikoj mjeri oslanja na računala i računalne mreže. Takvi sustavi olakšavaju i pospješuju rad organizacija, ali nesumnjivo unose i visok stupanj rizika. Računalna mreža i entiteti koji se njome koriste za međusobnu komunikaciju nužno uključuju određeni stupanj ranjivosti koje zlonamjerne osobe mogu iskoristiti. Moderni informacijski sustavi svakim danom postaju sve veći i kompleksniji te je iz tog razloga znatno otežan njihov nadzor i održavanje zadovoljavajuće razine sigurnosti u svim dijelovima.

Neke od mogućih posljedica pojave i eskalacije sigurnosnih propusta za organizaciju su:

- pad prihoda i gubitak poslovnih klijenata,
- smanjenje ugleda i reputacije tvrtke,
- narušavanje povjerenja partnera i klijenata,
- negativna medijska pozornost ili
- parničenje s pogođenim poslovnim subjektima.

Zato je razvijeno mnoštvo različitih sustava bodovanja ranjivosti. Ti sustavi identificiraju i procjenjuju ranjivosti različitih sklopovskih i programskih platformi. Pomoću njih se može odrediti prioritet ranjivosti i dati prednost onima koje predstavljaju veći rizik za organizaciju. Ali usprkos tome što su uvedeni sustavi bodovanja ranjivosti to nije u potpunosti riješilo probleme organizacija vezane uz sigurnosne ranjivosti. Razlog leži u tome što nije postojao jedinstven sustav bodovanja ranjivosti, pa je bilo gotovo nemoguće usporediti rizike koje pojedina ranjivost donosi. Javio se problem pretvaranja mnoštva podataka dobivenih različitim kriterijima bodovanja ranjivosti u neke korisne informacije primjenjive na svaku organizaciju. CVSS (eng. Common Vulnerability Scoring System) je otvoreno okruženje koje se bavi tim problemom. CVSS omogućava:

- **Standardizirano bodovanje ranjivosti:** Normalizacijom rezultata bodovanja ranjivosti za sva programska rješenja i sve sklopovske platforme može se uvesti jedinstvena politika upravljanja ranjivostima. Ta politika može biti ista kao i ugovor o razini usluge (eng. *service level agreement*) koji utvrđuje koliko brzo organizacija mora pronaći i ukloniti ranjivost.
- **Otvoreno okruženje** (eng. Open Framework): Korisnici mogu biti zbunjeni kada se ranjivost boduje na proizvoljan način jer tada ne mogu znati koja svojstva ranjivosti su dobila određene bodove. CVSS omogućuje prikaz svih individualnih svojstava korištenih za dobivanje rezultata.
- **Prioritet rizika** (eng. *Prioritized Risk*): Nakon izračunavanja rezultata u određenom okruženju, ranjivost postaje kontekstualna. Rezultati su sada reprezentativni i pokazuju stvarne rizike. Korisnicima postaje poznata važnost određene ranjivosti u odnosu na druge.

2. Common Vulnerability Scoring System

Sigurnost informacijskih sustava jedan je od glavnih problema, primarnih ciljeva i zaduženja svake organizacije. Zato se mnogo novca i vremena ulaže u postizanje što veće sigurnosti. Da bi se moglo pričati o sigurnosti prvo se moraju poznavati pojmovi koji će se provlačiti kroz cijeli tekst:

- **Ranjivost** – greška u programu, slabost, izloženost aplikacije, sustava, uređaja ili poslužitelja, koja može dovesti do propusta u povjerljivosti, integritetu ili dostupnosti podataka
- **Ugroženost** – mogućnost ili frekvencija pojavljivanja štetnog događaja.
- **Rizik** – relativni utjecaj ranjivosti na korisničko okruženje.

U povećanju sigurnosti informacijskih sustava veliku ulogu ima CVSS (eng. Common Vulnerability Scoring System) sustav. Radi se o nepristranom industrijskom standardu za ocjenjivanje ozbiljnosti sigurnosnih ranjivosti računalnog sustava. Korištenjem ovog sustava organizacije pokušavaju uspostaviti mjeru ozbiljnosti promatrane ranjivosti u usporedbi s drugim sličnim ranjivostima. Na temelju tih mjera uspostavljaju se prioriteti i određuje hitnost uklanjanja ranjivosti sustava. CVSS rješava problem mnogostrukih nekompatibilnih bodovnih sustava (npr. CERT/CC, SANS-ova skala ranjivosti, Microsoft-ov sustav bodovanja itd.). Lako je razumljiv i jednostavan za uporabu. Njegov kvantitativni model osigurava ponovljiva i točna mjerenja i omogućuje korisnicima uvid u svojstva ranjivosti koja su se koristila za oblikovanje rezultata. Rezultati se temelje na mnoštvu provedenih mjerenja (metrika) koja se temelje na stručnim procjenama. CVSS je zato prikladan kao standardizirani sustav mjerenja za industrije, organizacije i vlade koje trebaju točne i nepromjenjive rezultate utjecaja ranjivosti. Uobičajeno se upotrebljava za računanje ozbiljnosti ranjivosti pronađene u sustavu i određivanje prioriteta uklanjanja iste. Prihvaćanje zajedničkog jezika bodovanja ima veliku važnost za mnoge organizacije i donosi veliki dobitak IT menadžerima, analitičarima biltena ranjivosti, isporučiteljima sigurnosne opreme i aplikacija te istražiteljima.

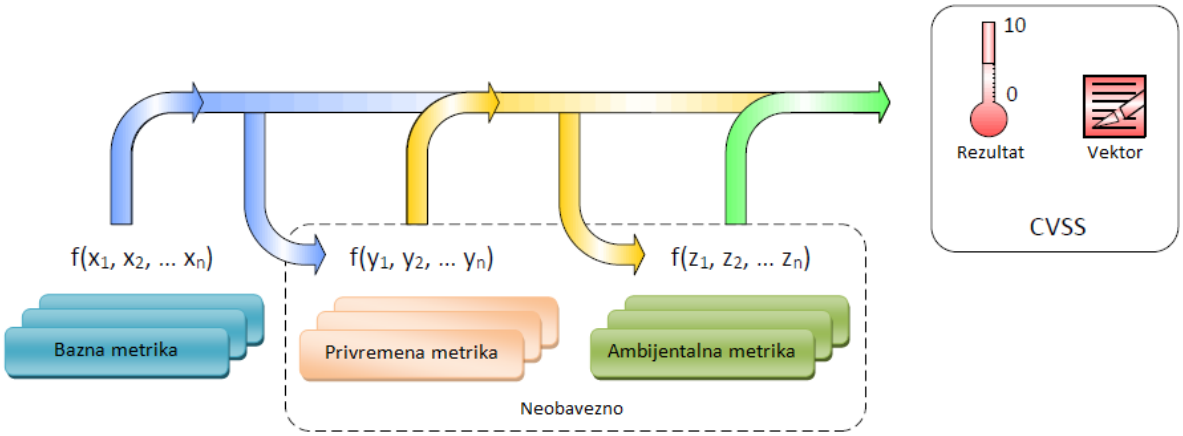
CVSS se sastoji od tri skupine metrika: bazne, privremene i ambijentalne, od kojih se svaka sastoji od serije utjecajnih podmetrika, kao što je prikazano na slici 1.

Slika 1. Metrike

Te tri različite skupine metrika ukratko se mogu definirati:

- **Bazna metrika (eng. *Base*)** - predstavlja bitne i temeljne osobine ranjivosti, nepromjenjive u vremenu i korisničkom okruženju.
- **Privremena metrika (eng. *Temporal*)** - predstavlja osobine ranjivosti koje se mijenjaju u vremenu, ali ne ovise o korisničkom okruženju.
- **Ambijentalna metrika (eng. *Environmental*)** - predstavlja osobine ranjivosti koje su bitne i jedinstvene u konkretnom korisničkom okuženju.

Bazna metrika definira komunikacijske i fundamentalne osobine ranjivosti. Ovaj objektivni pristup karakterizaciji ranjivosti korisnicima omogućuje jasan i intuitivan prikaz ranjivosti. Na temelju bazne metrike korisnici mogu primijeniti privremene i ambijentalne metrike i dobiti informacije koje točnije prikazuju rizik jedinstvenog korisničkog okruženja. Te novostečene korisne informacije omogućuju donošenje boljih odluka vezanih uz smanjivanje rizika uzrokovanih sigurnosnim propustima korisničkog sustava.



Slika 2. CVSS metrike i jednadžbe

Postoji mogućnost poboljšanja baznih rezultata dodjeljivanjem vrijednosti privremenim i ambijentalnim metrikama. Dobrim i detaljnim definiranjem ranjivosti smanjuju se rizici uzrokovani ranjivošću korisničke okoline. Bazni rezultati i vektori uglavnom su dovoljni za opis ranjivosti. Ako su za analizu ranjivosti sustava potrebni i privremeni rezultati, jednadžbe objedinjuju privremene metrike s baznim rezultatima. Tako se dobiju privremeni rezultati koji se izražavaju rasponom od 0 do 10. Na sličan način, ako je u određenom trenutku potreban rezultat okolinske metrike, okolinska jednadžba objedinjuje okolinsku metriku s rezultatima iz privremene metrike i kao rezultat također daje brojeve u rasponu od 0 do 10.

Vrijednosti bazne i privremene metrike uglavnom određuju analitičari biltena ranjivosti te isporučitelji opreme ili aplikacija. Oni uglavnom imaju bolje informacije o osobinama ranjivosti nego što ih imaju korisnici. Vrijednosti okolinske metrike određuju korisnici, jer oni mogu najbolje procijeniti potencijalni utjecaj ranjivosti na vlastiti informacijski sustav.

2.1. Razvoj

NIAC (eng. National Infrastructure Advisory Council) je razvio CVSS standard s ciljem potpore globalnom otkrivanju ranjivosti. Trenutno je CVSS pod skrbništvom organizacije FIRST (eng. Forum for Incident Response and Security Teams), koja je zadužena i za njegovo održavanje. Unatoč tome, CVSS je potpunosti besplatan i otvoren standard. Ni jedna organizacija nije vlasnik CVSS-a i zbog toga nije nužno biti član FIRST-a da bi koristili ili primjenjivali CVSS. Jedini zahtjev koji organizacije koje objavljuju rezultate moraju ispuniti jest da objavljeni rezultati moraju biti oblikovani prema propisanim smjernicama. Uz rezultate također moraju biti objavljeni i vektori rezultata. Tako svi zainteresirani mogu razumjeti način dobivanja rezultata ocjene pojedine ranjivosti. CVSS je nastao kao rezultat zajedničkog truda mnoštva organizacija, a neke od njih su:

- CERT/CC,
- Cisco,
- DHS/MITRE,
- eBay,
- IBM Internet Security Systems,
- Microsoft,
- Qualys i
- Symantec.

Nakon objavljivanja službene inačice CVSS-a, gore navedenim organizacijama pridružuju se i druge organizacije (Lumeta, CSC Australia, Mitre, BB&T, Webroot i druge) koje sudjeluju u izradi novih inačica CVSS standarda.

2.2. Primjena

Svakim danom povećava se broj korisnika CVSS-a. Svaka organizacija osjetljiva je na različite ranjivosti, a isto tako nisu svakoj organizaciji isti sigurnosni propusti jednako kritični. Nekima je najbitnija dostupnost, nekima pouzdanost i tako dalje. Svaka organizacija prilagođava CVSS vlastitim potrebama i rezultate tumači na drugačiji način. Bitno je napomenuti da su, bez obzira na to što su svi dobiveni na drugi način, rezultati normalizirani. Zahvaljujući normaliziranosti rezultata njihovo razumijevanje je jednostavno pa ih mogu razumjeti i analitičari svih drugih organizacija. Sve to dovelo je do rasta uporabe CVSS-a. U nastavku slijede primjeri nekih korisnika sustava bodovanja ranjivosti temeljenog na CVSS-u:

- **Isporučitelji izvješća o ranjivostima** (eng. *Vulnerability Bulletin Providers*): U besplatnim izvješćima o ranjivosti sustava neprofitne i komercijalne organizacije objavljuju CVSS bazne i privremene rezultate bodovanja ranjivosti. Izvješća nude mnoge informacije, uključujući i datume otkrivanja ranjivosti, ugrožene sustave, poveznice i preporučene načine uklanjanja ranjivosti.
- **Isporučitelji programskih aplikacija** (eng. *Software Application Vendors*): Isporučitelji programskih aplikacija također svojim korisnicima na uvid pružaju CVSS rezultate. Na taj način poboljšava se uvid u ozbiljnost sigurnosnih propusta koji se mogu pronaći u njihovim proizvodima. Korisnici tako mogu učinkovitije upravljati sigurnosnim rizicima.
- **Privatne tvrtke** (eng. *User Organizations*): Mnoge organizacije iz privatnog sektora interno koriste CVSS. Koriste ga za pravilno donošenje odluka u upravljanju ranjivostima. Skeneri ili tehnike nadgledanja prvo pronalaze ranjivost glavnog računala i aplikacija. Nakon toga primjenjuje se CVSS metrika za ocjenjivanje ranjivosti. Korisničke organizacije kombiniraju rezultate dobivene iz CVSS bazne, privremene ili okolne metrike kako bi dobile više podataka o kontekstualnom riziku i ranjivostima koje predstavljaju najveći rizik njihovom sustavu. Pri tome se svi korisnici vode logikom da se prvo uklanjaju ranjivosti najvišeg prioriteta.
- **Skeniranje i upravljanje ranjivostima** (eng. *Vulnerability Scanning and Management*): Organizacije koje se bave pronalaženjem i upravljanjem ranjivostima skeniraju mreže u potrazi za propustima u računalnim sustavima. One najčešće pružaju CVSS bazne rezultate za svaku ranjivost pojedinog računala. Korisničke organizacije koriste dobivene rezultate za još učinkovitije upravljanje vlastitim IT infrastrukturama. Reduciraju se gubici te se izvodi zaštita od zlonamjernih i slučajnih IT prijetnji.
- **Upravljanje sigurnosnim rizicima** (eng. *Security Risk Management*): Organizacije koje se bave upravljanjem sigurnosnim rizicima koriste CVSS rezultate kao ulazne vrijednosti za računanje razine rizika ili prijetnje. Te organizacije koriste napredne aplikacije, koje se često integriraju s njihovom mrežnom topologijom, ranjivim podacima i pružaju korisnicima bolje predodžbe o razinama rizika.

2.3. Inačice

FIRST je organizacija koja sponzorira i podupire CVSS-SIG (eng. *Common Vulnerability Scoring System-Special Interest Group*) grupu. CVSS-SIG čine razne organizacije koje svakodnevno koriste CVSS i profesionalno se bave sigurnošću pa imaju veliki interes za proučavanje sigurnosnih propusta. Mnogi članovi CVSS-SIG-a primjenjuju CVSS u vlastitim organizacijama. Njihovo iskustvo je pomoglo u oblikovanju predloženog smjera razvoja CVSS sustava pružajući neprekidno vodstvo u potpori i treniranju.

Postoje dvije inačice CVSS-a: CVSS v1 i CVSS v2. Nakon početne uporabe CVSS-a, koju su obavljale CVSS-SIG i druge organizacije pokazalo se da postoji mnoštvo značajnih problema s početnim konceptom CVSS-a (bazni rezultati nisu točno reflektirali stvarnu kritičnost ranjivosti, veća razilaženja u rezultatima od očekivanih, rezultati nisu bili dosljedni, a metrike dovoljno granularne). U želji da se pronađu najveći problemi i poveća točnost CVSS-a, CVSS-SIG počinje bilježiti ranjivosti, uspoređivati rezultate, pregledavati nedosljednosti te stvarati izmjene i dopune kojima se pronađeni nedostaci popravljaju. Kada je CVSS-SIG postigao dogovor oko određenog problema ili potencijalnog unapređenja, organizacije su glasale za odobrenje, odbacivanje ili slanje ispravke nazad odboru na daljnje proučavanje.

Dugo istraživanje svih rubnih slučajeva i problema bodovanja dovelo je do mnoštva rasprava među različitim organizacijama koje čine CVSS-SIG. CVSS-SIG je osim bodovanja novih ranjivosti, retroaktivno bodovao i stare ranjivosti, što se pokazalo ključnim za određivanje stvarne važnosti ranjivosti. Bodovanje starih ranjivosti omogućilo je novoj inačici (v2) uspoređivanje utjecaja ranjivosti iz ˝stvarnog svijeta˝ i rezultata dobivenih u inačici v1. Povrh svega toga, SIG je skupio sve ranjivosti u bazu podataka NIST-a (http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2). Navedena baza podataka služi za razumijevanje i usporedbu s prvom inačicom, što dovodi do poboljšanja rezultata i potencijalnog uvođenja promjena na mjestima pronalaska problema.

Nova inačica CVSS-a (v2) inicirana je u travnju 2005. godine i nastavila se razvijati sve do lipnja 2007. godine, kada je objavljena službena inačica. Na izgradnji nove inačice radila je grupa CVSS-SIG uz pomoć NIST-a (eng. National Institute of Standards and Technology). NIST je osigurao skupinu statistika koja se bavila proračunima kojima su se smanjivale nedosljednosti u korištenim formulama uključujući zaokruživanje, nedostatak raščlanjivosti rezultata, multiplikativna rješenja jednadžbi, probleme visoke sigurnosti i mnoge druge. Organizacija je napisala mnoštvo dokumentacije i inačica nacrta. CVSS-SIG je koristio nove formule u želji dobivanja bolje raširenosti, a u isto vrijeme i povećanja točnosti rezultata.

2.4. Drugi sustavi bodovanja ranjivosti

Naravno uz CVSS postoje i mnogi drugi sustavi bodovanja ranjivosti. Tim sustavima upravljaju i profitne i neprofitne organizacije. Svaki od njih ima svoja individualna postignuća i oni se međusobno razlikuju po načinu mjerenja ranjivosti sustava.

- Na primjer organizacija CERT/CC (eng. Computer Emergency Response Team Coordination Center) pruža numerički sustav bodovanja. Bodovanje je u tom sustavu u rasponu od 0 do 180. Pri bodovanju u obzir se uzimaju i mogućnost postojanja rizika vezanih uz internetsku infrastrukturu i preduvjeti potrebni za istraživanje ranjivosti.
- SANS-ova (eng. SysAdmin, Audit, Network, Security) skala ranjivosti uzima u obzir i nedostatke pronađene u zadanim postavkama ili klijentskom programskom sustavu.
- Microsoftov sustav bodovanja pokušava prikazati i poteškoće iskorištavanja i utjecaja ranjivosti na sustav.

Iako su jako korisni, navedeni sustavi bodovanja provode pristup ˝jedna procjena za sve˝, vodeći se pretpostavkom da je utjecaj ranjivosti konstantan za svakog individualnog korisnika ili cijelu organizaciju (što u većini situacija nije slučaj).

Kao što je već navedeno CVSS je nepristrani industrijski standard za ocjenjivanje ozbiljnosti sigurnosnih ranjivosti računalnog sustava, ali isto tako CVSS možemo definirati i poznavajući ono što on nije:

- Sustavi procjene, poput onih koje koristi DHS (eng. US Department of Homeland Security) i SANS-ov ISC (eng. Sans Internet Storm Center), koji osiguravaju savjetodavni sustav upozorenja vezanih uz prijetnje globalnim IT mrežama.
- Baza ranjivosti poput NVD (eng. National Vulnerability Database) i OSVDB (eng. Open Source Vulnerability Database) baze ili BugTraq-a. Navedene baze ranjivosti pružaju uvid u sve poznate ranjivosti i detalje vezane uz navedene ranjivosti.
- Identifikacijski sustav ranjivosti poput industrijskog CVE (eng. Common Vulnerabilities and Exposures) ili rječnika u kojem su navedene slabosti sustava, kao na primjer CWE rječnika (eng. Common Weakness Enumeration). Ova okruženja služe za jedinstvenu identifikaciju i klasifikaciju ranjivosti koje se pojavljuju u kodu, dizajnu ili arhitekturi.

3. Metrika CVSS-a

U osnovi metrike su mjerenja koja se temelje na stručnim procjenama. U narednim poglavljima opisane su metrike koje koristi CVSS sustav.

3.1. Bazna metrika

Bazna metrika bavi se osobinama ranjivosti koje su nepromjenjive u vremenu i u korisničkom okruženju. Vektor pristupa, složenost pristupa i autentikacijska metrika bilježe načine iskorištavanja ranjivosti. Oni označavaju da li su potrebni dodatni zahtjevi za istraživanje ranjivosti. Te tri utjecajne metrike mjere utjecaj ranjivosti (ako ona postoji) direktno na IT aktive. Utjecaji su neovisno definirani kao stupanj gubitka povjerljivosti, integriteta i dostupnosti. Na primjer, ranjivost može uzrokovati djelomični gubitak integriteta i dostupnosti, ali ne i gubitak povjerljivosti.

3.1.1. Vektor pristupa

Vektor pristupa izražava način iskorištavanja ranjivosti. Postoji tri vrijednosti koje ova metrika može poprimiti:

- lokalna mreža (eng. *Local*),
- susjedna mreža (eng. *Adjacent Network*) ili
- mreža (eng. *Network*)

Pri ocjenjivanju vrijednosti metrike gleda se udaljenost zlonamjernog korisnika od njegove mete napada. Što je udaljenost veća, veći je i rezultat koji obilježava ranjivost.

Vrijednost metrike	OPIS
Lokalni	Ranjivosti koje zlonamjerni korisnici mogu iskorištavati samo lokalnim pristupom zahtijevaju postojanje fizičkog pristupa ranjivom sustavu ili posjedovanje lokalnog korisničkog računa (eng. *local/shell account*). Primjeri lokalno iskoristivih ranjivosti su periferni napadi poput: Firewire/USB DMA napad ili LPE (eng. *local privilege escalations*).
Susjedni	Ranjivosti iskoristive samo sa susjednim pristupom zahtijevaju mogućnost pristupa domeni prostiranja (eng. *broadcast domain*) ili domeni kolizije (eng. *collision domain*) ranjivog programskog paketa. Primjeri susjednih mreža su: lokalna IP podmreža, Bluetooth, IEEE 802.11 i lokalni Ethernet.
Mrežni	Ranjivosti iskoristive mrežnim pristupom koriste komunikaciju putem mrežnih protokola (eng. *network stack*). Zlonamjernim korisnicima zbog toga nije potreban pristup lokalnoj mreži ili lokalni pristup. Primjer mrežnog napada je RPC prepisivanje spremnika (eng. *RPC buffer overflow*).

Tablica 1. Bodovanja vektora pristupa

3.1.2. Složenost pristupa

Složenost pristupa je metrika koja mjeri potrebnu složenost napada zlonamjernog korisnika s ciljem iskorištavanja ranjivosti sustava. Napad može započeti tek kada je napadač dobio pristup sustavu kojega je želio napasti. Na primjer, neka se za primjer uzme napad koji koristi preljev spremnika na poslužitelju davatelja internetskih usluga. Tek nakon što je napadač pronašao ciljni sustav, može mu pristupiti i iskoristi ga. Isto tako, ako promatramo ranjivost elektronske pošte, ona se može iskoristiti samo nakon što korisnik preuzme i otvori zaraženi privitak. Ova metrika može poprimiti nekoliko različitih vrijednosti:

- visoka složenost,
- srednja složenost i
- niska složenost.

Što je manja potrebna složenost pristupa, veća je iskoristivost ranjivosti.

Vrijednost metrike	OPIS
Visoka	Postoje specijalizirani uvjeti pristupa: • Da bi napadač izveo napad na nekog korisnika u većini konfiguracija on mora unaprijed imati veće privilegije ili dodatne sustave za varanje. • Napad ovisi o metodama socijalnog inženjeringa koje obrazovani ljudi mogu lako prepoznati. Na primjer, žrtva napada mora izvesti nekoliko sumljivih i atipičnih radnji. • Ranjiva konfiguracija rijetko je uočiva u praksi. • Ako postoje još neki dodatni uvjeti, mogućnost pristupa je jako mala.
Srednja	Uvjeti pristupa su donekle specijalizirani. Neki primjeri su: • Napadač je ograničen. Ima samo određenja ovlaštenja pri pristupu skupini sustava ili korisnika. • Neke informacije moraju biti prikupljene prije izvođenja uspješnog napada. • Konfiguracija na koju napadač ima utjecaj nije standardizirana i nije u potpunosti konfigurirana (npr. ranjivost postoji kada poslužitelj preko specifičnih shema provjerava korisnički račun, ali nije prisutna pri nekim drugim shemama). • Napad zahtjeva malo socijalnog inženjeringa, kojim se povremeno može zavarati i oprezni korisnik.
Niska	Ne postoje specijalni uvjeti pristupa ili olakšavajuće okolnosti pristupa. Slijede neki primjeri: • Produkt na koji se pokušava utjecati najčešće zahtjeva pristup mnoštvu sustava i korisnika koji su eventualno anonimni i nepouzdani (npr. internet pristup *web* ili *mail* poslužitelju) • Pogođena konfiguracija je standardna ili svuda prisutna. • Napad može biti obavljen ručno, što zahtjeva malo vještine i prikupljanja potrebnih informacija. • Za obavljanje napada nisu potrebne velike vještine, napad se lako izvršava.

Tablica 2. Bodovanja složenosti pristupa

3.1.3. Autentikacija

Ova metrika mjeri koliko puta napadač mora dokazati svoju autentičnost pri pristupu meti kako bi iskoristio njenu ranjivost. Metrika ne mjeri snagu ili složenost autentikacijskog procesa, već samo koliko puta napadač mora proći određene akreditacije prije nego što dobije mogućnost iskorištavanja ranjivosti. Metrika provjere može poprimiti sljedeće vrijednosti:

- višestruka autentikacija
- jednostruka autentikacija ili
- „bez autentikacije“.

Što je manji broj puta u kojima zlonamjerni korisnik mora potvrditi svoju vjerodostojnost, to je veći utjecaj ranjivosti na sustav.

Autentikacijska metrika nije isto što i vektor pristupa, pogotovo za lokalno iskoristive ranjivosti. Ova metrika trebala bi poprimiti vrijednosti ˝jednom˝ i ˝višestruko˝ ako je autentikacija potrebna, a ˝nijednom˝ ako se ne obavlja provjera pri pristupu.

Vrijednost metrike	OPIS
Višestruka	Iskorištavanje ranjivosti zahtjeva autentikaciju zlonamjernog korisnika najmanje dva puta. Pri autentikaciji ponekada se u svakom pokušaju pristupa koriste isti podaci.
Jednostruka	Potrebna je samo jedna autentikacija za pristup i iskorištavanje ranjivosti.
Nije potrebna	Za pristup i iskorištavanje ranjivosti nije potrebna autentikacija.

Tablica 3. Bodovanje autentikacije

Ova metrika bi se trebala upotrebljava samo na temelju autentikacije napadača prije izvođenja napada, odnosno provjerava se da li se da li i koliko se puta mora provesti postupak autorizacije. Na primjer, ako je udaljeni *mail* poslužitelj osjetljiv na naredbe koje se zadaju prije autentikacije, rezultat metrike bi trebao biti ˝nije potrebna˝ jer napadač može dobiti pristup i iskoristiti ranjivost prije zahtjeva za upisivanje podataka vezanih uz autentikaciju. Ako je sustav ranjiv samo nakon uspješne autentikacije, tada bi rezultat ove metrike trebao glasiti ˝višestruka˝ ili ˝jednostruka˝.

3.1.4. Utjecaj na povjerljivost

Ova metrika mjeri utjecaj na povjerljivost podataka koji se mogu otkriti. Povjerljivost se odnosi na ograničavanje pristupa i otkrivanje informacija samo ovlaštenim korisnicima, kao i na zabranu pristupa i otkrivanja informacija neovlaštenim. Vrijednosti koje ova metrika može poprimiti su:

- nepostojeći utjecaj na povjerljivost,
- djelomični utjecaj na povjerljivost ili
- potpuni utjecaj na povjerljivost.

Vrijednost metrike	OPIS
Nepostojeći	Ne postoji utjecaj na povjerljivost podataka u sustavu
Djelomični	Postoji znatno otkrivanje informacija. Moguć je pristup samo određenim datotekama, ali napadač nema nadzor nad time koje informacije može dobiti ili nad razmjerom gubitka nadzora. Koristan primjer utjecaja na povjerljivost je ranjivost koja otkriva samo određene tablice ili baze podataka.
Potpuni	Otkrivanje svih datoteka sustava rezultira potpunim otkrivanjem svih informacija. Napadač je u mogućnosti pročitati sve datoteke sustava (uključujući i memoriju, arhive...)

Tablica 4. Bodovanje utjecaja na povjerljivost

3.1.5. Utjecaj na integritet

Ova metrika mjeri utjecaj na integritet uspješno iskorištene ranjivosti. Integritet se odnosi na pouzdanost i zagarantiranu istinitost informacija. Vrijednosti koje ova metrika može poprimiti su:

- nepostojeći utjecaj na integritet,
- djelomični utjecaj na integritet i
- potpuni utjecaj na integritet.

Povećanjem utjecaja na integritet raste i utjecaj ranjivosti na sustav.

Vrijednost metrike	OPIS
Nepostojeći	Ne postoji utjecaj na integritet podataka u sustavu
Djelomični	Postoji mogućnost modifikacije nekih sistemskih datoteka ili informacija, ali napadač pri tome nema nadzor nad time što može biti promijenjeno i ograničen je opseg područja na koja zlonamjerni korisnik može utjecati. Na primjer, napadač može prepisati ili promijeniti datoteke sustava ili aplikacijske datoteke, ali pri tome on ne može sam birati koje će datoteke brisati i/ili promijeniti.
Potpuni	Dolazi do potpunog kompromisa integriteta sustava. Sustav više nije zaštićen, zbog čega je cijeli sustav ugrožen. Napadač može izmijeniti svaki podatak na napadnutom računalu.

Tablica 5. Bodovanje utjecaja na integritet

3.1.6. Utjecaj na dostupnost

Ova metrika mjeri utjecaj ranjivosti na dostupnost podataka . Dostupnost se odnosi na pristupačnost informacijskih resursa. Napadi koji koriste širinu pojasa mreže, cikluse procesora ili prostor na disku i time utječu na dostupnost sustava. Vrijednosti koje ova metrika može poprimiti su:

- nepostojeći utjecaj na dostupnost,
- djelomični utjecaj na dostupnost i
- potpuni utjecaj na dostupnost

Vrijednost metrike	OPIS
Nepostojeći	Ne postoji utjecaj na dostupnost podataka u sustavu
Djelomični	Smanjeno je djelovanje sustava, odnosno pojavljuju se prekidi u dostupnosti resursa. Primjer je: *network-based flood* napad koji dopušta samo određeni broj uspješnih spajanja.
Potpuni	Dolazi do potpunog prekida rada napadnutih resursa. Napadač resurse može prikazati potpuno nepristupačnima.

Tablica 6. Bodovanje utjecaja na dostupnost

3.2. Privremena metrika

Prijetnja uzrokovana ranjivošću nekoga sustava može se tokom vremena mijenjati. Tri faktora, na temelju kojih CVSS sustav izvršava bodovanje su: potvrda tehničkih detalja ranjivosti, status otklanjanja ranjivosti te dostupnost koda za iskorištavanje ranjivosti (eng. *exploit*) i tehnika. Kako su privremene metrike neobavezne, njihovi rezultati nemaju utjecaja na konačni rezultat. Vrijednosti dobivene ovom metrikom se koriste kada korisnik smatra da određena metrika nije dovoljno dobra za određivanje ranjivosti specifičnih sustava i želi ju preskočiti.

3.2.1. Iskoristivost

Ova metrika mjeri trenutno stanje korištenih tehnika iskorištavanja ranjivosti ili dostupnost koda. Javna dostupnost koda za iskorištavanje ranjivosti dovodi do povećanja broja potencijalnih napadača, na taj način povećavajući ozbiljnost ranjivosti. Iskoristivosti iz ˝stvarnog svijeta˝ su samo teorijske. Objavljivanjem tzv. *proof od concept* koda (sinonim za zero-day exploit kod, kod koji ne iskorištava u potpunosti određenu ranjivost), *functional exploit* (kod koji u potpunosti iskorištava određenu ranjivost) koda ili dovoljno tehničkih detalja omogućava lakše iskorištavanje ranjivosti. Iz dostupnog *proof-of-concept* koda može se razviti *exploit* kod koji je onda uspješan u iskorištavanju

ranjivosti. *Exploit* kod u obliku korisnog sadržaja dolazi do korisničkog računala uz pomoć zlćudnog programa ili crva. Vrijednosti koje ova metrika može poprimiti su:

- nedokazana iskoristivost,
- *Proof-of-Concept* iskoristivost,
- funkcionalna iskoristivost,
- visoka iskoristivost i
- nedefinirana iskoristivost.

Što zlonamjerni korisnik lakše iskorištava ranjivost sustava, veći je utjecaj ranjivosti na sustav.

Vrijednost metrike	OPIS
Nedokazana	Iskoristivi kod nije dostupan ili je iskorištavanje u potpunosti teorijsko.
Proof-of-Concept	Dostupan je *proof-of-concept* kod ili demonstracija napada, koja nije praktična za većinu sustava. Kod ili tehnika nije funkcionalna u svim sustavima i od vještog napadača zahtijeva značajne promjene.
Funkcionalna	Dostupan je funkcionalni kod za iskorištavanje. Kod radi u većini situacija u kojima postoje ranjivosti.
Visoka	Ranjivost se iskorištava uz pomoć samostalnog mobilnog koda ili nije potrebno iskorištavanje (ručni okidač). Kod je primjenjiv u svakoj situaciji ili se aktivno dostavlja uz pomoć anonimnog mobilnog agenta (crv ili zlćudni program).
Nedefinirana	Dodjeljivanje vrijednosti metrici neće utjecati na rezultat. To je signal jednadžbi koji označava preskakanje ove metrike.

Tablica 7. Bodovanje iskoristivosti

3.2.2. Stupanj ispravljanja ranjivosti

Stupanj ispravljanja ranjivosti je jako važan faktor pri određivanju prioriteta. Tipična ranjivost nije ispravljena u trenutku kada je objavljena. Izbjegavanje ranjivosti ili brzi popravci mogu poslužiti kao privremena rješenja, sve do službenog popravka ili nadogradnje rješenja koje uklanja prvotni problem. Svaki od tih odgovarajućih popravaka smanjuje rezultate privremene metrike. Povećanjem broja popravaka smanjuje se hitnost i rezultat. Dakle, što je veća hitnost popravka, privremeni rezultati su viši, a povećavanjem broja popravaka privremeni rezultat se smanjuje. Konačni popravak ranjivosti daje najmanji rezultat privremenoj metrici.

Vrijednost metrike	OPIS
Službeni popravak	Isporučitelj je izdao potpuni službeni ispravak ili je dostupna nadogradnja.
Privremeni popravak	Dostupan je službeni, ali samo privremeni ispravak. To uključuje slučajeve kada isporučitelj izdaje privremeni brzi popravak, alat ili zaobilaznicu.
Izbjegavanje	Dostupno je rješenje koje nije izdao isporučitelj. U tom slučaju korisnici zaražene tehnologije samostalno stvaraju put ili korake kako bi zaobišli ranjivost ili ju umanjili.
Nedostupni	Ne postoji dostupno rješenje ili ga je nemoguće primijeniti.
Nedefinirani	Dodjeljivanje ove vrijednosti metrici neće utjecati na rezultat. To je signal jednadžbi za preskakanje promatrane metrike.

Tablica 8. Bodovanje razina popravaka

3.2.3. Pouzdanost izvješća

Ova metrika mjeri stupanj povjerljivosti pri postojanju ranjivosti i vjerodostojnost poznatih tehničkih detalja. Ponekad organizacije objavljuju samo činjenicu da ranjivosti postoje, ali ne i bitne detalje vezane uz ranjivost. Ranjivost se može kasnije potkrijepiti i nakon toga potvrditi uz pomoć autora ili izdavača programskog paketa. Hitnost ispravljanja ranjivosti je veća ako je sa sigurnošću poznato postojanje ranjivosti. Ova metrika također ukazuje na razinu tehničkog znanja dostupnu napadačima. Što više izdavača ili drugih izvora potvrdi postojanje ranjivosti, to ona ima veći rezultat.

Vrijednost metrike	OPIS
Nepotvrđena	Postoji jedan nepotvrđen izvor ili nekoliko proturječnih izvješća. Malo je povjerenje u vjerodostojnost izvješća. Primjer je glasina koja kruži iz okoline zlonamjernog napadača.
Nepotkrijepljena	Postoji mnoštvo neslužbenih izvora, koji ponekada uključuju i nezavisne sigurnosne ili istraživačke organizacije. Zahvaljujući tome postoji mogućnost postojanja suprotstavljenih tehničkih detalja ili trajnih dvosmislenosti.
Potvrđena	Izdavač ili autor zaražene tehnologije potvrdio je postojanje ranjivosti. Ranjivost također može biti potvrđena objavljivanjem *functional* ili *proof-of concept* koda ili jako raširenog iskorištavanja.
Nedefinirana	Dodjeljivanje ove vrijednosti metrici neće utjecati na rezultat. To je signal za preskakanje promatrane metrike.

Tablica 9. Bodovanje pouzdanosti izvješća

3.3. Ambijentalna metrika

Sustavi mnogih organizacija podložni su različitim rizicima. CVSS ambijentalna metrika boduje osobine ranjivosti koje su povezane s korisničkim IT okruženjem. Kako okolinske metrike nisu obavezne, one daju rezultate koji nemaju utjecaja na općeniti rezultat. Ova metrika uzima u obzir okolinska testiranja sustava.

3.3.1. Usporedni potencijal štete

Ova metrika mjeri mogućnost prestanka rada sustava ili nestanka fizičkih dobara uzrokovanu oštećenjem ili krađom imovine ili opreme. Metrika može mjeriti i ekonomski gubitak produktivnosti. Vrijednosti koje može poprimiti su:

- nema štete,
- mala šteta,
- mala-srednja šteta,
- srednja-velika šteta,
- velika šteta i
- nedefinirana šteta.

Naravno, što je veći potencijal štete, veći je i njen utjecaj na sustav.

Vrijednost metrike	OPIS
Nepostojeća	Ne postoji mogućnost prestanka rada, gubitka fizičkih dobara, produktivnosti ili prihoda.
Niska	Iskorištavanje ove ranjivosti može dovesti do maloga gubitka fizičkih dobara ili određenih svojstava.
Niska-srednja	Uspješno iskorištavanje ranjivosti rezultira umjerenom fizičkom ili nekom drugom štetom. Može se pojaviti i umjereni gubitak dobitka ili prihoda u organizaciji.
Srednje-visoka	Uspješno iskorištavanje ranjivosti rezultira značajnom fizičkom ili nekom drugom štetom. Može se pojaviti i umjereni gubitak dobitka ili prihoda u organizaciji.
Visoka	Uspješno iskorištavanje ranjivosti rezultira katastrofalnim fizičkom ili nekom drugom štetom. Može se pojaviti i kobni gubitak dobitka ili prihoda u organizaciji.
Nedefinirana	Dodjeljivanje ove vrijednosti metrici neće utjecati na rezultat. To je signal za preskakanje promatrane metrike.

Tablica 10. Bodovanje potencijala štete

3.3.2. Distribucija ranjivosti

Ova metrika mjeri udio ranjivog sustava u cjelokupnom sustavu. Ona je posebni ambijentalni indikator, koji pokazuje koliki je dio sustava na koji bi ranjivost mogla utjecati. Vrijednosti koje ova metrika može poprimiti su:

- nepostojeća distribucija ranjivosti u sustavu,
- mala distribucija ranjivosti u sustavu,
- srednja distribucija ranjivosti u sustavu,
- velika distribucija ranjivosti u sustavu ili
- nedefinirana distribucija ranjivosti u sustavu.

Što je veći udio ranjivosti u sustavu, to je veći utjecaj ranjivosti.

Vrijednost metrike	OPIS
Nepostojeća	Ne postoje ugroženi dijelovi sustava ili su oni usko specijalizirani, toliko da postoje samo u laboratoriju (0% okoline izloženo je riziku).
Niska	Postoje ranjivi dijelovi okoline, ali su jako mali. Riziku je izloženo samo 1-25% okoline.
Srednja	Postoje ranjivi dijelovi okoline, ali su srednje veličine. Riziku je izloženo 26-75% okoline.
Visoka	Ranjivi dijelovi imaju jako veliki udio u cjelokupnom sustavu. Riziku je izloženo 76-100% okoline.
Nedefinirana	Dodjeljivanje ove vrijednosti metrici neće utjecati na rezultat. To je signal jednadžbi za preskakanje promatrane metrike.

Tablica 11. Bodovanje distribucije ranjivosti

3.3.3. Zahtjevi sigurnosti

Zahvaljujući ovoj metrici analitičari mogu prilagođavati CVSS rezultate. Rezultati se prilagođavaju ovisno o važnosti zaraženog dijela IT imovine za pojedinu organizaciju. Važnost se mjeri ovisno o povjerljivosti, integritetu i dostupnosti. Na primjer, ako je za pojedinu organizaciju dostupnost

najvažniji dio informacijskih tehnologija, analitičari mogu dodijeliti veću vrijednost dostupnosti u odnosu na povjerljivost i integritet. Svaki zahtjev sigurnosti može imati tri vrijednosti:

- niski zahtjev sigurnosti ,
- srednji zahtjev sigurnosti i
- visoki zahtjev sigurnosti.

Na vrijednosti rezultata ambijentalne metrike utjecaj imaju odgovarajuće bazne metrike. Bazne metrike mijenjaju ovaj rezultat ponovnim mjerenjem baznih metrika povjerljivosti, integriteta ili dostupnosti. Da bi se to lakše objasnilo koristi se sljedeći primjer. Ako je zahtjev za povjerljivost visok, povećati će se vrijednost metrike povjerljivosti. Na isti način smanjena je vrijednost rezultata metrike povjerljivosti ako je nizak zahtjev za povjerljivost. Do promjena vrijednosti ne dolazi ako je ″djelomični″zahtjev za povjerljivost. Iste logike se primjenjuju za integritet i dostupnost.

Ako je rezultat metrike povjerljivosti postavljen u ″nepostojeći″ tada zahtjevi povjerljivosti neće imati utjecaja na konačni rezultat. Kada bazna metrika ima vrijednost ″potpuni″, povećanje zahtjeva povjerljivosti sa ″srednji″ na ″visoki″ neće promijeniti okolinske rezultate. Razlog tome je već najveća moguća vrijednost rezultata metrike povjerljivosti.

Moguće vrijednosti zahtjeva sigurnosti nalaze se u tablici 12. Navedena tablica koristi se za sve tri metrike. Što su zahtjevi za sigurnost viši, to je rezultat veći.

Vrijednost metrike	OPIS
Niski	Gubitak [povjerljivosti | integriteta | dostupnosti] ima samo mali ili ograničeni utjecaj na organizaciju ili individualce povezane s organizacijom (poslodavci, zaposlenici).
Srednji	Gubitak [povjerljivosti | integriteta | dostupnosti] ima ozbiljno štetan utjecaj na organizaciju ili individualce povezane s organizacijom (poslodavci, zaposlenici).
Visoki	Gubitak [povjerljivosti | integriteta | dostupnosti] ima potpuno štetan utjecaj na organizaciju ili individualce povezane s organizacijom (poslodavci, zaposlenici).
Nedefinirana	Dodjeljivanje ove vrijednosti metrici neće utjecati na rezultat. To je signal jednadžbi za preskakanje promatrane metrike.

Tablica 12. Bodovanje zahtjeva sigurnosti

4. Bazni, privremeni i ambijentalni vektori

Svaki vektor sastoji se od skraćenog imena metrike. Nakon imena metrike slijedi ″:″ (dvotočka), a nakon nje skraćena vrijednost metrike. U vektoru su unaprijed određenim redoslijedom izlistane vrijednosti metrike. Znak ″/″ koristi se za razdvajanje metrika. Ako se ne koriste privremena ili ambijentalna metrika, pridružuje im se vrijednost ″nedefinirana″.

Bazna metrika sastoji se od sljedećih metrika, koje mogu poprimiti različite vrijednosti navedene u nastavku:

- Vektor pristupa - lokalni, susjedna mreža, mreža (VP:[L,SM,MR])
- Složenost pristupa - visoka, srednja, mala (SP:[V,S,M])
- Autentikacija - višestruka, jednom, nije potrebna (Au:[VS,J,N])
- Utjecaj na povjerljivost - nepostojeći, djelomični, potpuni (P:[NP,D,PT])
- Utjecaj na integritet - nepostojeći, djelomični, potpuni (I:[NP,D,PT])
- Utjecaj na dostupnost - nepostojeći, djelomični, potpuni (D:[NP,D,PT])

Privremena metrika sastoji se od sljedećih metrika, koje mogu poprimiti različite vrijednosti navedene u nastavku:

- Iskoristivost - nedokazana, *Proof-of-Concept, f*unkcionalna, visoka, nedefinirana (IS:[ND,POF,F,V,NF])
- Stupanj ispravljanja ranjivosti - službeni popravak, privremeni popravak, izbjegavanje, nedostupni, nedefinirani (IR:[SP,PP,IZ,NS,NF])
- Pouzdanost izvješća - nepotvrđena, nepotkrijepljena, potvrđena, nedefinirana (PI:[NT,NK,PV,NF])

Ambijentalna metrika sastoji se od sljedećih metrika, koje mogu poprimiti različite vrijednosti navedene u nastavku:

- Usporedni potencijal štete - nepostojeći, niski, niski-srednji, srednji-visoki, visoki i nedefinirani (PS:[NP,N,N-S,S-V,V,NF])
- Distribucija ranjivosti - nepostojeća, niska, srednja, visoka, nedefinirana (DR:[NP,N,S,V,NF])
- Zahtjevi sigurnosti - niski, srednji, visoki, nedefinirani (ZS:[NP,N,S,V,NF])

U Tablici (13) prikazan je način pisanja baznog, privremenog ili ambijentalnog vektora. U zagradama su navedene vrijednosti koje pojedina metrika može poprimiti, a znakom ″/″ su razdvojene metrike.

Metrika	Vektor
Bazna	VP:[L,SM,MR]/SP:[V,S,M]/Au:[VS,J,N]/P:[NP,D,PT]/ I:[NP,D,PT]/I:[NP,D,PT]/D:[NP,D,PT]: [L,A,N]/AC:[H,M,L]/ Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Privremena	IS:[ND,POF,F,V,NF]/IR:[SP,PP,IZ,NS,NF]/PI:[NT,NK,PV,NF]
Ambijentalna	PS:[NP,N,NS,SV,V,NF]/DR:[NP,N,S,V,NF]/ZS:[NP,N,S,V,NF]

Tablica 13. Bazni, privremeni i ambijentalni vektori

Da bi se zornije predočili vektori navodi se sljedeći primjer. Ranjivost daje vrijednosti baznoj metrici: ″Vektor pristupa:lokalni; Složenost pristupa: srednja; autentikacija: nije potrebna; Utjecaj povjerljivosti: nepostojeći; Utjecaj integriteta: djelomični; Utjecaj na dostupnost: potpuni″. Ranjivost bi tada imala sljedeći bazni vektor: ″VP:L/SP:S/Au:N/P:NP/I:D/P:PT″

Vektor pristupa:	lokalni
Složenost pristupa:	srednja
Autentikacija:	nije potrebna
Utjecaj povjerljivosti:	nepostojeći
Utjecaj integriteta:	djelomični
Utjecaj na dostupnost:	potpuni

Tablica 14. Primjer bodovanja ranjivosti

Vektor:	AV:L/AC:M/Au:N/C:N/I:P/A:C.

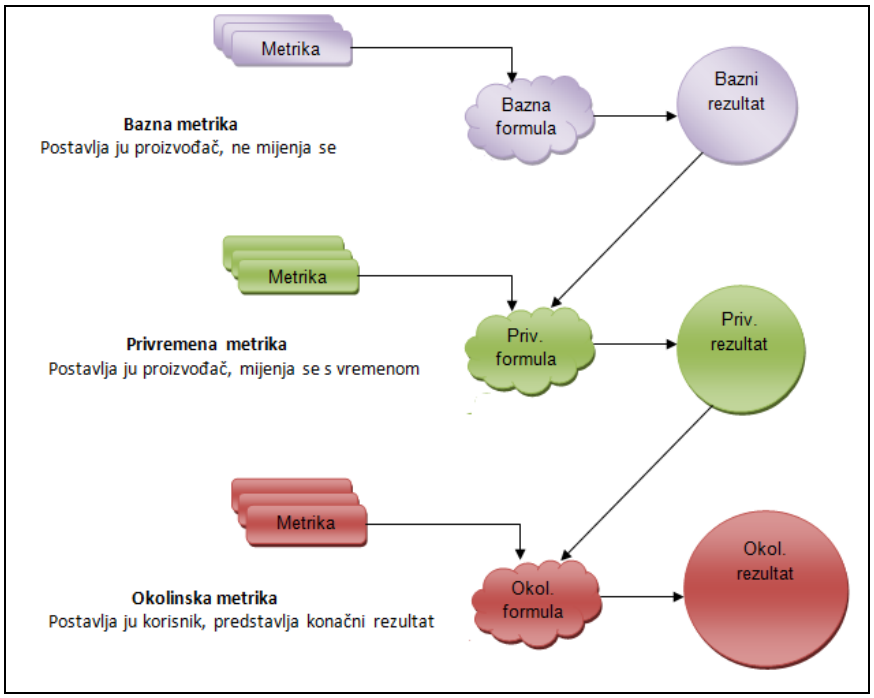
Tablica 15. Bazni vektor

5. Bodovanje

Bodovanje je proces povezivanja vrijednosti svih metrika uz pomoć specifičnih formula. Bodovanje bazne metrike provodi proizvođač ili organizator s namjerom objave rezultata koji se ne mijenjaju. Rezultati se računaju iz tri metrike: povjerljivosti, integriteta i dostupnosti. To je funkcija čije rezultate mogu promijeniti utjecaji privremene i okolinske metrike. Bazni rezultat ima najveći utjecaj na konačni rezultat i on najvećim dijelom reprezentira kritičnost ranjivosti.

Proizvođači i koordinatori publikacije računaju privremene rezultate. Privremena metrika može mijenjati vrijednost baznoj metrici. Privremeno bodovanje dopušta uvođenje dodatnih faktora kojima se smanjuje rezultat ranjivosti. Privremeno bodovanje ranjivosti dizajnirano je tako da omogući ponovno ocjenjivanje ranjivosti u određenim vremenskim razmacima. Privremeni rezultat predstavlja hitnost popravljanja ranjivosti u posebnim vremenskim trenucima.

Okolinsko bodovanje mogu provoditi korisničke organizacije. Bodovanje prilagođava bazno-privremene rezultate. Dobiveni rezultati mogu se smatrati konačnim rezultatom, koji predstavlja snimak u vremenu, napravljen u određenoj okolini. Korisničke organizacije bi trebale koristiti ovo bodovanje kako bi odredile prioritete u vlastitom okruženju.



Slika 3 Bodovanje

Postoje određene smjernice koje mogu pomoći analitičarima pri bodovanju ranjivosti. Te smjernice su:

- opće smjernice,
- bazna metrika,
- autentikacija i
- utjecaj na povjerljivost integriteta i dostupnost

Smjernice su detaljnije objašnjene u nastavku teksta.

5.1. Općenite smjernice

- **TIP 1**: Pri bodovanju ranjivosti u obzir se ne bi trebalo uzeti međudjelovanje s drugim ranjivostima. Svaka ranjivost bi se trebala neovisno bodovati.
- **TIP 2**: Pri bodovanju ranjivosti razmatra se samo izravni utjecaj na ciljano glavno računalo. Na primjer neka se razmotri XSS (eng. *cross-site scripting*) ranjivost. XSS je tehnika zlonamjernih napada kojom napadač uspije potaknuti korisnički web preglednik na izvođenje podmetnutog programskog koda, što mu omogućava da prikupi različite osjetljive podatake dostupne putem web preglednika. Utjecaj XSS ranjivosti na korisnički sustav mogao bi biti puno veći od utjecaja na ciljani web poslužitelj, ali to je indirektan utjecaj. Pri bodovanju se promatraju samo direktni utjecaji. XSS ranjivost bi trebala biti bodovana bez utjecaja na povjerljivost ili dostupnost i djelomični utjecaj na integritet.
- **TIP 3**: Mnoge aplikacije (npr. web poslužitelji) izvode se korištenjem različitih povlastica. Nije uvijek poznato koje su povlastice korištene pri stvaranju određene aplikacije. Zato se bodovanje izvodi sa pretpostavljanjem korištenih povlastica. To naravno nije najbolji način što se tiče sigurnosti, pogotovo za aplikacije koje se izvode uz pomoć administratorskih ovlasti. Ponekada analitičari ne mogu biti sigurni koje su ovlasti korištene. U tom slučaju bi trebali pretpostaviti uobičajenu konfiguraciju.
- **TIP 4**: Zlonamjerni korisnici često mogu jednu ranjivost iskorištavati na različite načine. Kada se jedna ranjivost iskorištava na više načina analitičari bi pri bodovanju trebali izabrati metodu iskorištavanja koja ima najveći utjecaj, a ne metodu koja je najčešća ili najlakša za provođenje. Na primjer, ako postoji *functional* kod za jednu platformu, ali ne i za drugu, tada bi iskoristivost trebala imati vrijednost: ˝funkcionalna˝. Ako se paralelno razvijaju dvije različite inačice proizvoda, a popravljena je samo jedna inačica, količina popravaka trebala biti postavljena u ˝nedostupni˝, dakle pri bodovanju uvijek se uzima najgori slučaj.

5.2. Bazna metrika

5.2.1. Vektor pristupa

- **TIP 5**: Kada zlonamjerni korisnici ranjivost mogu iskoristiti i lokalno i preko mreže, treba se izabrati vrijednost ˝mreža˝. Kada ranjivost može biti iskorištena lokalno i preko susjedne mreže, ali ne i preko svih mreža, vrijednost mora biti postavljena u ˝susjedna mreža˝. Kada se ranjivost može iskoristiti i preko susjedne mreže i preko javne mreže (Interneta) treba se izabrati vrijednost ˝mreža˝.
- **TIP 6**: Mnoge korisničke aplikacije i uslužni programi imaju razne lokalne ranjivosti. Te lokalne ranjivosti zlonamjerni korisnici mogu iskorištavati i udaljeno uz pomoć automatske analize i nekih pomoćnih aplikacija. Sljedeći primjer to pobliže objašnjava. Programi za dekompresiju i skeneri zloćudnih programa automatski skeniraju dolazeću elektroničku poštu. Kada se zaražene datoteke dijele korištenjem „mail“ komunikacije ili preuzimaju preko web stranica iskorištavaju se i pomoćne aplikacije. Analitičari bi takve pristupne vektore trebali bodovati kao ˝mreža˝.

5.2.2. Autentikacija

- **TIP 7:** Ranjivost se može pojaviti u samom planu provjere ili u anonimnom poslužitelju. Vrijednost metrike tada bi trebala biti: ˝nije potrebna autentikacija˝ jer napadač može iskoristiti ranjivost bez pružanja ikakvih valjanih identifikacijskih podataka (iako ih možda i

posjeduje). Prisutnost uobičajenog korisničkog imena može se smatrati kao ˝jednostruka˝ ili ˝višestruka˝ prijava. Pri tome dolazi do objave identifikacjiskih podataka i iskoristivost se postavlja u ˝velika˝.

5.2.3. Utjecaj povjerljivosti, integriteta i dostupnosti

- **TIP 8**: Ranjivosti koje zlonamjernim korisnicima omogućavaju pristup administratorskoj (*root)* razini boduju se kao potpuni gubitak povjerljivosti, integriteta i dostupnosti. Ranjivosti koje daju pristup korisničkoj razini bi se trebale bodovati kao djelomični gubitak povjerljivosti, integriteta i dostupnosti. Na primjer, narušavanje integriteta koje zlonamjernim korisnicima dozvoljava promjenu lozinki operacijskog sustava trebalo bi se bodovati kao ˝potpuni˝ gubitak povjerljivosti, integriteta i dostupnosti.
- **TIP 9**: Ranjivosti koje uzrokuju potpuni gubitak integriteta mogu imati utjecaj i na dostupnost. To se može vidjeti u sljedećem primjeru. Ako napadač u potpunosti iskorištava ranjivost nekoga sustava on može dobiti pristup sistemskim datotekama, može mijenjati njihov sadržaj ili ih brisati. Na taj način zlonamjerni korisnik uzrokuje velike štete korisnicima ili organizacijama, jer manipulira njihovim podacima i računalima na kojima se nalaze. Zlonamjerni korisnik može otkriti neke tajne podatke, manipulirati financijskim sredstvima, mijenjati sadržaj nekih bitnih datoteka. Organizacije tada mogu izgubiti kredibilitet kod svojih korisnika, izgubiti mnogo novaca, može im usporiti razvoj i sl.

5.3. Jednadžbe

Jednadžbe i algoritmi uz pomoć kojih se boduju bazne, privremene i okolinske metrike su navedene u nastavku teksta.

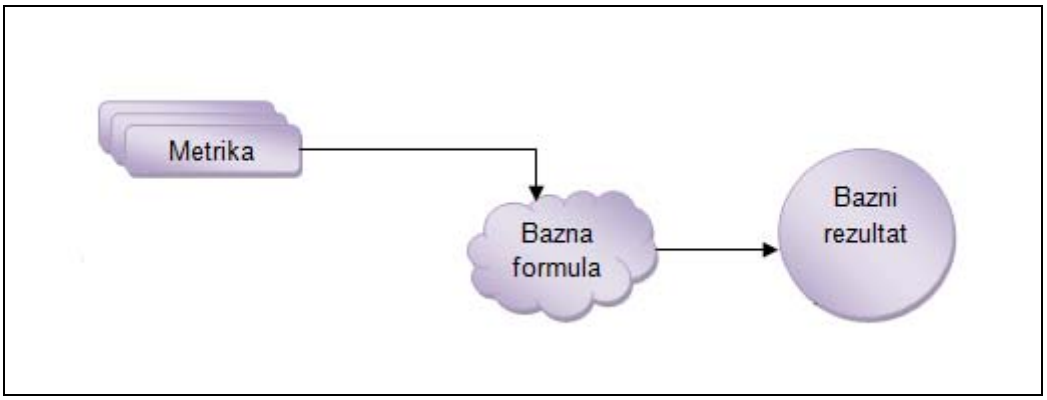
5.3.1. Jednadžba baze

CVSS sustav računa rezultat baze na temelju šest kriterija, odnosno baznih metrika. Bazni rezultat se odnosi na osnovne, nepromjenjive osobine ranjivosti. Kriteriji koji oblikuju bazni rezultat su:

- **Vektor pristupa** - Mjeri koliko napadač mora biti udaljen da bi izvršio napad. Vrijednosti koje može poprimiti su: lokalni, susjedna mreža, mreža.
- **Složenost pristupa** - Mjeri potrebnu složenost napada s kojom bi se mogla iskoristiti ranjivost sustav. Vrijednosti koje može poprimiti su: visoka, srednja, mala.
- **Autentikacija** - Mjeri koliko puta napadač mora izvršiti autentikaciju pri pristupu meti. Vrijednosti koje može poprimiti su: višestruka, jednom, ni jednom.
- **Utjecaj na povjerljivost** - Ova metrika mjeri utjecaj na povjerljivost podataka koji se mogu otkriti. Vrijednosti koje može poprimiti su: nepostojeći, djelomični, potpuni.
- **Utjecaj na integritet** - Mjeri koliki je utjecaj ranjivosti na povjerljivost podataka. Vrijednosti koje može poprimiti su: nepostojeći, djelomični, potpuni.
- **Utjecaj na dostupnost** - Ova metrika mjeri utjecaj ranjivosti na dostupnost podataka. Vrijednosti koje može poprimiti su: nepostojeći, djelomični, potpuni.

Svaki od tih šest kriterija može poprimiti tri različite vrijednosti. Ovisno o karakteristikama ranjivosti dodjeljuju se numeričke vrijednosti svakoj od tri moguće vrijednosti pojedinog kriterija. Nakon toga bazna jednadžba se koristi za dodjeljivanje težine svakome kriteriju, povezivanje dobivenih vrijednosti i dobivanje konačnog baznog rezultata.

U starijoj inačici CVSS-a bazni rezultat se računao samo na na temelju metrika. U drugoj inačici te se metrike dijele u dvije grupe: metrike utjecaja i poteškoća. U novoj inačici bazne jednadžbe se dijele u dvije pod-jednadžbe, svaka za pojedinu grupu metrika. Za svaku jednadžbu CVSS-SIG je analizirao relativnu važnost svake moguće kombinacije metrika i razvio je pravila koja objašnjavaju rezultate analiza



Slika 4. Bodovanje bazne metrike

Jednadžba baze ima sljedeći oblik:

BazniRezultat = round_to_1_decimal(((0.6*Utjecaj)+(0.4*Iskoristivost)– 1.5)*f(Utjecaj))

Utjecaj= 10.41*(1-(1-Povjerljivosti)*(1-Integritet)*(1-Dostupnosti))

Iskoristivost = 20* VektorPristupa*SlozenostPristupa *Autentikacija

f(Utjecaj) = 0 if Utjecaj=0, 1.176 otherwise

VektorPristupa = case VektorPristupa of
Lokalni pristup: 0.395
Susjedna mreza: 0.646
mreza: 1.0

SlozenostPristupa = case SlozenostPristupa of
visok: 0.35
srednji: 0.61
mala: 0.71

Autentikacija = case Autentikacija of
Visestruka autentikacija: 0.45
Jednostruka Autentikacija: 0.56
Autentikacija nije potrebna: 0.704

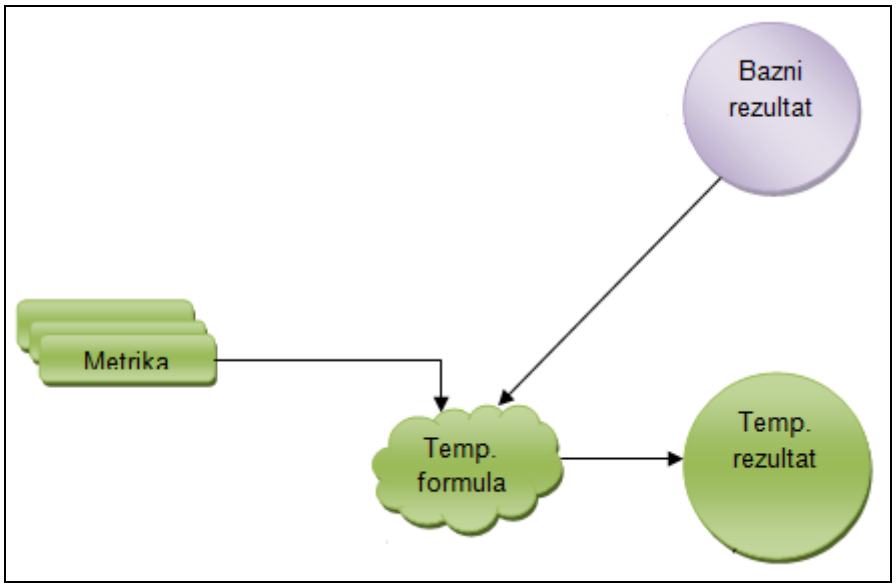
Povjerljivost = case UtjecajNaPovjerljivost of
nepostojeci: 0.0
djelomicni: 0.275
potpuni: 0.660

Integritet = case UtjecajNaIntegritet of
nepostojec
djelomicni: 0.275
potpuni: 0.660

Dostupnost = case UtjecajNaDostupnost of
nepostojeci: 0.0
djelomicni: 0.275
potpuni: 0.660

5.3.2. Privremena jednadžba

Ponekad metrika baze ne daje zadovoljavajuće rezultate, pa je potrebno koristiti i privremenu metriku. Ako je potrebno, privremena jednadžba spaja privremenu metriku s baznim rezultatom kako bi se dobio privremeni rezultat. Rezultat može poprimiti vrijednosti u rasponu od 0 do 10. Privremeni rezultat ne može biti viši od rezultata baze, a ne može biti manji od 33% rezultata baze.



Slika 5. Bodovanje privremene metrike

Privremena jednadžba definirana je na sljedeći način:

PrivremeniRezultat = round_to_1_decimal(BazniRezultat*Iskoristivost *IspravakRanjivosti*PouzdanostIzvjesca)

Iskoristivost = case Iskoristivost of
nedokazan: 0.85
proof-of-concept: 0.9
funkcionalna: 0.95
visok: 1.00
nedefiniran: 1.00

IspravakRanjivosti = case IspravakRanjivosti of
Sluzbeni popravak: 0.87
Privremeni popravak: 0.90
izbjegavanje: 0.95
nedostupan: 1.00
nedefiniran: 1.00

PouzdanostIzvjesca = case PouzdanostIzvjesca of
nepotvrdena: 0.90
nepotkrijepljena: 0.95
potvrdena: 1.00
nedefinirana: 1.00

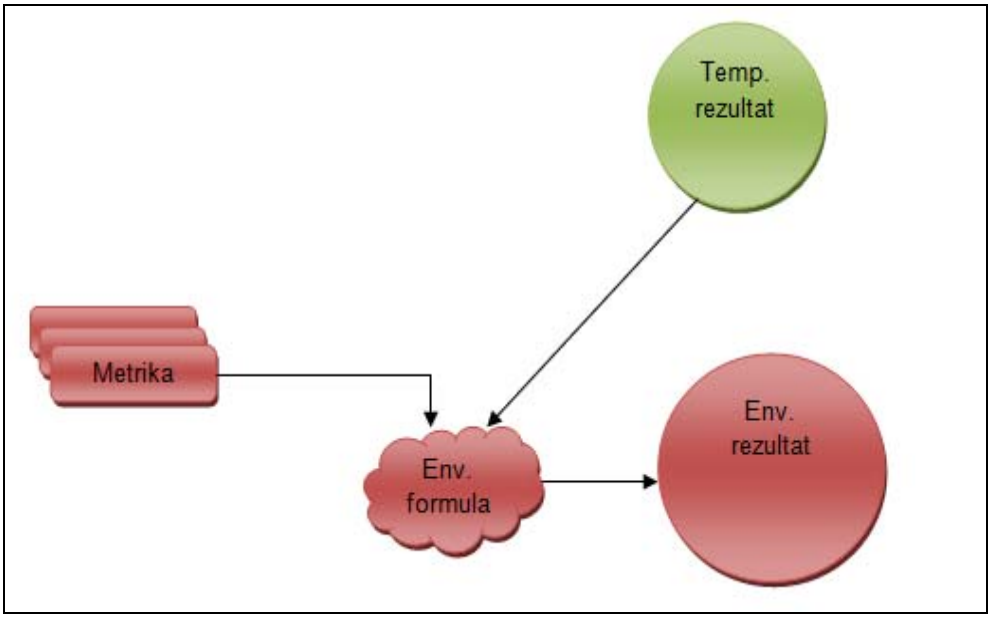
5.3.3. Ambijentalna jednadžba

Ambijentalno bodovanje ranjivosti sustava mogu provoditi sami korisnici. Ambijentalnim bodovanjem se prilagođavaju bazno-privremeni rezultati. Rezultat navedenog postupka je konačni rezultat, koji predstavlja ranjivost specifične okoline.

Ambijentalna metrika boduje ranjivosti povezane s korisničkim okruženjem. Metrika koje oblikuju ambijentalni rezultat su:

- Usporedni potencijal štete - mjeri mogućnost prestanka rada sustava ili nestanka fizičkih dobara. Vrijednosti koje ova metrika može poprimiti su: nepostojeći, niski, niski-srednji, srednji-visoki, visoki i nedefinirani.
- Distribucija ranjivosti - mjeri udio ranjivog sustava u cjelokupnom sustavu. Vrijednosti koje ova metrika može poprimiti su: nepostojeća,niska, srednja, visoka, nedefinirana
- Zahtjevi sigurnosti - služi za prilagodbu rezultata ovisno o povjerljivosti, integritetu i dostupnosti. Vrijednosti koje ova metrika može poprimiti su: niski, srednji, visoki, nedefinirani.

Svaki od tih navedenih kriterija može poprimiti različite vrijednosti. Ovisno o karakteristikama ranjivosti dodjeljuju se numeričke vrijednosti svakoj od mogućih vrijednosti pojedine metrike. Nakon toga ambijentalna jednadžba dodjeljivanje težine svakome kriteriju povezuje rezultate dobivene ambijentalnim metrikama s privremenim rezultatom. Jednadžba na kraju daje konačan ambijentalni rezultat. Rezultat može imati raspon od 0 do 10. Rezultat dobivene jednadžbe ne smije biti viši od privremenog rezultata.



Slika 6. Bodovanje ambijentalne metrike

Jednadžba ima sljedeći oblik:

AmbijentalniRezultat = Round_to_1_decimal((PrilagodenPrivremeni+(10-PrilagodenPrivremeni)*PotencijalStete) *DistribucijaRanjivosti)

PrilagodenPrivremeni = PrivremeniRezultat ponovo se racuna s BazniRezultat utjecajnom podjednadzbom zamijenjenom s PrilagodenImpact jednadzbom

PrilagodenUtjecaj = min(10,10.41*(1-(1-ConfImpact*ZahtjevPovjerljivosti)*(1-UtjecajIntegriteta*IntegReq)*(1-UtjecajDostupnosti*ZahtjevDostupnosti)))

PotencijalStete = case PotencijalStete of
nepostoji: 0

nizak: 0.1
nizak-srednji: 0.3
srednji-visok: 0.4
visok: 0.5
nedefiniran: 0

DistribucijaRanjivosti = case DistribucijaRanjivosti of
nepostoji: 0
nizak: 0.25
srednji: 0.75
visok: 1.00
nedefiniran: 1.00

ZahtjevPovjerljivosti = case ZahtjevPovjerljivosti of
nizak: 0.5
srednji: 1.0
visok: 1.51
nedefiniran: 1.0

ZahtjevIntegriteta= case ZahtjevIntegriteta of
nizak: 0.5
srednji: 1.0
visok: 1.51
nedefiniran: 1.0

ZahtjevDostupnosti = case ZahtjevDostupnosti of
nizak: 0.5
srednji: 1.0
visok: 1.51
nedefiniran: 1.0

5.4. Primjeri

CVSS se zbog svog načina rada može primjenjivati na mnoge različite ranjivosti. U tekstu koji slijedi navedeni su neki primjeri ranjivosti.

5.4.1. CVE-2002-0392

Da bi lakše mogli razumjeti rad CVSS-a i razloge njegove uporabe promotrit u nastavku će biti prikazana ranjaviosto Apache web poslužitelja - „Apache Chunked-Encoding Memory Corruption" , koja je otkrivena 2002. godine. Unutar Apache web poslužitelja pronađen je sigurnosni nedostatak koji omogućava napade sa udaljenih lokacija. Nedostatak se nalazi unutar mehanizma za rukovanjem "chunked" paketima prilikom prihvaćanja klijentskih podataka nepoznate duljine. Uspješno iskorištavanje ranjivosti može dovesti do odbijanja usluge ili napadač sa udaljene lokacije omogućiti izvođenje proizvoljnog programskog koda.

Navedenu ranjivost zlonamjerni korisnici mogu iskorištavati s udaljenih lokacija pa vektor pristupa ima vrijednost: ˝mreža˝. Nisu potrebne nikakve posebne okolnosti za uspješno iskorištavanje ranjivosti. Složenost pristupa je ˝niska˝, i napadač za uspješno iskoriptavanje treba samo umetnuti pažljivo oblikovanu poruku Apache web poslužitelju. Autentikacija nije potrebna za iskorištavanje ranjivosti (svaki korisnik Interneta može se povezati na web poslužitelj) pa je vrijednost autentikacijske metrike ˝nije potrebna provjera˝.

Naravno, ranjivost se može iskorištavati korištenjem mnoštva različitih metoda, koje daju različite vrijednosti izlaza. Bodovanje se provodi za svaku metodu, a kao izlazna vrijednost se uzima najveća vrijednost dobivena bodovanjem svake metode pojedinačno.

Ako je uz dozvolu web poslužitelja moguće pokrenuti proizvoljni programski kod i na taj način mijenjati web sadržaj ili je moguće promatrati lokalne korisnike s ciljem iskorištavanja ranjivosti

njihovih sustava, vrijednost metrika utjecaja na povjerljivost i integritet bi trebala biti: ˝djelomičan˝. Zajedno te dvije metrike daju bazi vrijednost 6.4.

Ako se ranjivost iskorištava kao odbijanje usluge, utjecaj na dostupnosti je ˝potpuni˝. Zajedno metrike daju rezultat baze 7.8. Kako je to najveći mogući rezultat koji mogu dati opcije iskorištavanja, on se koristi kao konačni rezultat baze.

REZULTAT BAZNE METRIKE

Vektor pristupa[Mreza] (1.00)
Slozenost pristupa[Niska] (0.71)
Autentikacija [Nepostojeca] (0.704)
Utjecaj na povjerljivost[Nepostojeci] (0.00)
Utjecaj na integritet[Nepostojeci] (0.00)
Utjecaj na dostupnost[Potpuni] (0.66)

FORMULA BAZNOG REZULTATA

Utjecaj = 10.41*(1-(1)*(1)*(0.34)) == 6.9
Iskoristivost = 20*0.71*0.704*1 == 10.0
f(Utjecaj) = 1.176
BazniRezultat = (0.6*6.9 + 0.4*10.0 – 1.5)*1.176
== (7.8)

REZULTAT PRIVREMENE METRIKE

Iskoristivost [Funkcionalna] (0.95)
IspravakRanjivosti[Sluzbeni-popravak] (0.87)
PouzdanostIzvjesca[Potvrdjena] (1.00)

FORMULA PRIVREMENOG REZULTATA

---

round(7.8 * 0.95 * 0.87 * 1.00) == (6.4)

REZULTAT AMBIJENTALNE METRIKE

PotencijalStete[Nepostojeci - Visoki] {0 - 0.5}
DistribucijaRanjivosti[Nepostojeci - Visoki] {0 - 1.0}
ZahtjevPovjerljivosti[Srednji] (1.0)
ZahtjevIntegriteta[Srednji] (1.0)
ZahtjevDostupnosti[Visoki] (1.51)

FORMULA AMBIJENTALNOG REZULTATA

PrilagodeniUtjecaj = min(10,10.41*(1-(1-0*1)*(1-0*1)

```
*(1-0.66*1.51)) == (10.0)
PrilagodeniBazni =((0.6*10)+(0.4*10.0)–1.5)*1.176
== (10.0)
PrilagodeniPrivremeni == (10*0.95*0.87*1.0) == (8.3)
AmbijentalniRezultat = round((8.3+(10-8.3)*{0-0.5})*{0-1})
== (0.00 - 9.2)
---------------------------------------------------
```

5.4.2. CVE-2003-0818

Drugi primjer jest ranjivost *„Microsoft Windows ASN.1 Library Integer Handling“*, otkrivena 2003. godine. Uspješnim iskorištavanjem ranjivosti dolazi do prepisivanja memorijskog spremnika. Zlonamjernim korisnicima to daje mogućnost izvođenja proizvoljnog koda s administrativnim ovlastima.

Navedenu ranjivost zlonamjerni korisnici mogu iskoristiti i udaljeno, zbog toga je vrijednost vektora pristupa ˝mreža˝ (VP:MR), a autentikacije ˝nije potrebna˝. Za uspješnost iskorištavanje nisu potrebne nikakve dodatne specijalne okolnosti niti posebni načini pristupa, pa je vrijednost autentikacije ˝nije potrebna˝, što složenosti pristupa daje vrijednost ˝mala˝ (SP:M). Zbog mogućnosti potpunog kompromisa sustava sve su metrike utjecaja (metrike utjecaja na povjerljivost, integritet i dostupnost) postavljene u ˝potpuni˝ (P:PT/I:PT/D:PT). Zajedno te metrike daju rezultat 10.

Vektor baze ima vrijednost

BAZNI VEKTOR	VP:MR/SP:M/Au:N/P:PT/I:PT/D:PT

Tablica 17. Vrijednost baznog vektora

Ova ranjivost je i dalje iskoristiva, pa je iskoristivost ˝funkcionalna˝ (IS:F). Microsoft je 2004. godine objavio popravak MS04-007. Popravljena inačica promijenila je vrijednosti metrike popravaka u ˝službeni popravak˝ (IR:SPP)i povjerljivosti izvješća je ˝potvrđena˝ (PI:PV). Privremeni rezultat je zbog toga postaje 8.3.

PRIVREMENI VEKTOR	IS:F/IR:SPP/PI:PV

Tablica 18. Vrijednost privremenog vektora

Pretpostavimo da je dostupnost važan čimbenik organizacije. Ovisno o vrijednostima posrednog potencijala štete i distribucije ranjivosti, rezultat ambijentalne metrike poprima vrijednosti u rasponu od 0.0 do 9.0. U nastavku slijedi konačni rezultat.

Neka se pretpostavi da su povjerljivost, integritet i dostupnost približno jednako važne za sustav pa ovisno o iznosu potencijala štete i distribuciji ranjivosti okolinski rezultat može imati vrijednosti u rasponu od 0 do 7.5.

REZULTAT BAZNE METRIKE

Vektor pristupa[Mreza] (1.00)
Slozenost pristupa[Niska] (0.71)
Autentikacija [Nepostojeca] (0.704)
Utjecaj na povjerljivost[Potpuni] (0.66)
Utjecaj na integritet[Potpuni] (0.66)
Utjecaj na dostupnost[Potpuni] (0.66)

FORMULA BAZNOG REZULTATA

Utjecaj = 10.41*(1-(0.34*0.34*0.34)) == 10.0
Iskoristivost = 20*0.71*0.704*1 == 10.0
f(Utjecaj) = 1.176
BazniRezultat =((0.6*10.0)+(0.4*10.0)–1.5)*1.176
== (10.0)

REZULTAT PRIVREMENE METRIKE

Iskoristivost [Funkcionalna] (0.95)
IspravakRanjivosti[Sluzbeni-popravak] (0.87)
PouzdanostIzvjesca[Potvrdjena] (1.00)

FORMULA PRIVREMENOG REZULTATA

---

round(10.0 * 0.95 * 0.87 * 1.00) == (8.3)

REZULTAT AMBIJENTALNE METRIKE

PotencijalStete[Nepostojeci - Visoki] {0 - 0.5}
DistribucijaRanjivosti[Nepostojeci - Visoki] {0 - 1.0}
ZahtjevPovjerljivosti[Srednji] (1.0)
ZahtjevIntegriteta[Srednji] (1.0)
ZahtjevDostupnosti[Niski] (0.5)

FORMULA AMBIJENTALNOG REZULTATA

PrilagodeniUtjecaj = 10.41*(1-(1-0.66*1)*(1-0.66*1)
*(1-0.66*0.5)) == 9.6
PrilagodeniBazni =((0.6*9.6)+(0.4*10.0)–1.5)*1.176
== (9.7)
PrilagodeniPrivremeni == (9.7*0.95*0.87*1.0) == (8.0)
AmbijentalniRezultat = round((8.0+(10-8.0)*{0-0.5})*{0-1})
== (0.00 - 9.0)

5.4.3. CVE-2003-0062

Posljednji primjer prikazuje preljev spremnika u antivirusnom programu NOD32. NOD32 je antivirusni program koji je razvila tvrtka Eset. Ranjivost je otkrivena 2003. godine u Linux i Unix inačicama, u inačicama starije od (uključivo) 1.013. Lokalni korisnici su mogli izvesti *proizvoljni* kod s privilegijama običnog korisnika. Tek nakon što je neki drugi korisnik obavio skeniranje svoga sustava, napadač je mogao početi iskorištavati ranjivost.

Ranjivost sustava je moguće iskoristiti samo preko lokalno prijavljenog korisnika. Vrijednost vektora pristupa je ˝lokalni˝ (VP:L). Zlonamjerni korisnik ne može iskorištavati ranjivosti sustava kada poželi pa je složenost pristupa ˝velika˝ (SP:V), tj. napadač mora pričekati odeđenu akciju drugog korisnika. Ta činjenica napadu daje dodatnu razinu složenosti. Zlonamjerni korisnik se ne mora prijavljivati i niti jednom dodatno obaviti autentikaciju, pa provjera vjerodostojnosti ima vrijednost ˝nije potrebna˝ (Au:N). Ako korisnik, koji je administrator sustava, sam uzrokuje preljev spremnika, napadač može u potpunosti kompromitirati sustav. Kod promatranja utjecaja ranjivosti na sustav uvijek se u obzir uzima najgori slučaj. U ovom primjeru svaka je metrika utjecaja postavljena na ˝potpuni˝ utjecaj (P:PT/I:PT/D:PT). Zajedno ove metrike proizvode rezultat baze u iznosu 6.2.

Vektor baze promatrane ranjivosti ima vrijednost:

BAZNI VEKTOR	VP:L/SP:V/Au:N/P:PT/I:PT/D:PT

Tablica 19. Vrijednost baznog vektora

Javno je dostupan samo djelomični *exploit* kod. Metrika iskoristivosti je postavljena u ˝*Proof-Of-Concept*˝ (I:POC). Eset je objavio obnovljenu inačicu svoga programa, što je razini popravaka dalo vrijednost ˝službeni popravak˝ (IR:SP) i povjerljivosti izvještaja je ˝potvrđena˝ (PI:PT). Ove tri metrike prilagođavaju rezultat baze da bi se dobio *temporal* rezultat 4.9.U nastavku slijedi konačni rezultat.

PRIVREMENI VEKTOR	IS:POC/IR:SPP/PI:PV

Tablica 20. Vrijednost privremenog vektora

REZULTAT BAZNE METRIKE

Vektor pristupa[lokalni] (0.395)
Slozenost pristupa[Visoka] (0.35)
Autentikacija [Nepostojeca] (0.704)
Utjecaj na povjerljivost[Potpuni] (0.66)
Utjecaj na integritet[Potpuni] (0.66)
Utjecaj na dostupnost[Potpuni] (0.66)

FORMULA BAZNOG REZULTATA

Utjecaj = 10.41*(1-(0.34*0.34*0.34)) == 10.0
Iskoristivost = 20*0.35*0.704*0.395 == 1.9
f(Utjecaj) = 1.176
BazniRezultat =((0.6*10)+(0.4*1.9)–1.5)*1.176 == (6.2)

REZULTAT PRIVREMENE METRIKE

Iskoristivost [Proof-Of-Concept](0.90)
IspravakRanjivosti[Sluzbeni-popravak] (0.87)
PouzdanostIzvjesca[Potvrdjena] (1.00)

FORMULA PRIVREMENOG REZULTATA

---

round(6.2 * 0.90 * 0.87 * 1.00) == (4.9)

REZULTAT AMBIJENTALNE METRIKE

PotencijalStete[Nepostojeci - Visoki] {0 - 0.5}
DistribucijaRanjivosti[Nepostojeci - Visoki] {0 - 1.0}
ZahtjevPovjerljivosti[Srednji] (1.0)
ZahtjevIntegriteta[Srednji] (1.0)
ZahtjevDostupnosti[Srednji] (1.0)

FORMULA AMBIJENTALNOG REZULTATA

PrilagodeniPrivremeni == 4.9
AmbijentalniRezultat = round((4.9+(10-4.9)*{0-0.5})*{0-1})
== (0.00 - 7.5)

---

6. Budućnost

Prva inačica CVSS otvorenog standarda za ocjenjivanje ozbiljnosti sigurnosnih ranjivosti računalnog sustava bila je CVSS v1. Razvoj prve inačice je počeo u srpnju 2003., a završio u siječnju 2004. godine. Ta inačica nije bila dovoljno dobra jer je postojalo mnoštvo značajnih problema u početnom konceptu CVSS-a (najvećim dijelom u sustavu ocjenjivanja pojedinog elementa ranjivosti). Naravno, ti problemi morali su biti ispravljeni. Analitičari su uskoro počeli nadopunjavati tadašnju inačicu, bilježiti ranjivosti i uspoređivati rezultate, pregledavati nedosljednosti i stvarati izmjene i dopune kojima su se nedostaci popravljali. Proces nastanka nove inačice započeo je 2005. godine, a završio je u 2007. godini. Nova se inačica pokazala znatno boljom od prethodne. To je dovelo do sve veće primjene CVSS-a u raznim drugim organizacijama. Prednost ovoga sustava bodovanja ranjivosti je u tome što on daje standardizirane rezultate koje mogu razumjeti i analitičari iz drugih organizacija. Zahvaljujući tome sve više organizacija počinje upotrebljavati ovaj sustav ranjivosti, jer uz pomoć njega mogu lako razumjeti i uspoređivati rezultate s drugim organizacijama. Naravno, svakim danom pojavljuju se nove ranjivosti i novi problemi u sigurnosti, tako da će se i trenutna inačica sigurno naći pred određenim problemima, koje će analitičari morati ispraviti. Neke od stvari koje će se mijenjati u novoj inačici su: metrika potencijala štete moći će mjeriti i financijsku štetu koju ranjivost nanosi organizaciji, ocjenjivati će se koliko je jednostavno izvršiti napad na korisnika kada već postoji *exploit* kod (do sada se mjerilo samo koliko je teško napisati kod), ranjivosti uz pomoć kojih se pristupa korijenskim datotekama imat će vrijednost ˝potpuni utjecaj˝, postoje još mnoge stvari koje će se s vremenom mijenjati u ovome sustavu bodovanja itd. Tako će se pojavljivati nadopune trenutne, a nakon nekog vremena sigurno i nova inačica ovog sustava bodovanja ranjivosti. CVSS će sigurno i u budućnosti biti jedan od najvažnijih standarda bodovanja ranjivosti i povećati će se broj organizacija koje ga primjenjuju zato što je lako dostupan, transparentan, jednostavan za korištenje i standardiziran.

7. Zaključak

U današnje vrijeme sigurnost informacijskih sustava jedan je od glavnih problema, primarnih ciljeva i zaduženja svake organizacije. Procjena rizika bitan je korak pri uspostavi sigurnosti informacijskih sustava. Važan dio upravljanja sigurnošću predstavlja upravljanje rizikom, odnosno uspostava odnosa između ranjivosti, potencijalnih prijetnji i posljedica, odnosno utjecaja na informacijski sustav. Proces upravljanja rizikom sastoji se od sljedećih koraka:

- identifikacije resursa,
- analize rizika,
- tumačenja rezultata i
- poduzimanja odgovarajućih protumjera

Mnoge organizacije zato svakodnevno ulažu velike količine novca kako bi si osigurale što veću sigurnost vlastitih sustava (jer se žele zaštiti od zlonamjernih napadača). Kada zlonamjerni napadači dobiju pristup sustavu, oni mogu mijenjati i preuzimati važne podatke i na taj način organizacijama prouzrokovati mnoge probleme i financijske gubitke. Zbog toga sve više različitih organizacija, ali i privatnih korisnika koristi sustave bodovanja ranjivosti. Mnoge od organizacija se pri izboru sustava bodovanja opredjeljuju za CVSS zato što žele dobiti rezultate koje će svi moći razumjeti, koji su standardizirani i koje će zbog toga moći lako uspoređivati s rezultatima drugih organizacija. Naravno nisu svakoj organizaciji iste ranjivosti jednako kritične, pa zbog toga CVSS omogućava svakoj organizaciji da ga prilagodi vlastitim potrebama. Nakon što se sustav prilagodi potrebama korisnika on pokušava uspostaviti mjeru ozbiljnosti ranjivost u usporedbi s drugim ranjivostima. Na temelju tih mjera uspostavljaju se prioriteti i određuje hitnost odgovora. Nakon što se ranjivost ukloni, do tada ugroženi podaci postaju sigurni i tako se smanjuje mogućnost gubitka podataka i financijskih sredstava. Mnoge su organizacije počele objavljivati CVSS rezultate, jer na takav način njihovi korisnici shvaćaju i cijene prednosti koje im nudi ta organizacija. Korisnicima je bitna povjerljivost podataka, učestalost napada, postoji li kod za iskorištavanje ranjivosti i još mnoge druge stvari. Promatrajući CVSS rezultate koje je objavila promatrana organizacija oni mogu uspoređivati različite organizacije, njihove ranjivosti i na taj način se lakše odlučiti s kojom će organizacijom surađivati. Objavljivanje rezultata bitno je i za organizacije i korisnike. Nakon što se korisnici odluče za određenu organizaciju oni mogu prilagoditi bodovanje ranjivosti prema vlastitim potrebama, odnosno prema vlastitom okruženju. Dugi sustavi bodovanja ranjivosti ne mogu bodovati ranjivosti u promjenjivim okruženjima i zato ne uzimaju u obzir različita okruženja. Ti sustavi nisu standardizirani i teško ih je razumjeti i gotovo nemoguće uspoređivati pomoću njih dobivene rezultate s rezultatima drugih sustava bodovanja, što korisnicima može prouzrokovati mnoge probleme. CVSS ima veliku prednost u odnosu na druge sustave jer je otvoreno okruženje koje je lako razumljivo i standardizirano. Svaki korisnik ga može lako koristiti, razumjeti i prilagoditi svojim potrebama.

8. Reference

[1] [1] Common Vulnerability Scoring System (CVSS-SIG),
http://www.first.org/cvss/

[2] [2] A complete Guide to the Common Vulnerability Scoring System Version 2.0,
http://www.first.org/cvss/cvss-guide.html

[3] [3] NVD Common Vulnerability Scoring System Support v2,
http://nvd.nist.gov/cvss.cfm

[4] [4] CVSS
http://en.wikipedia.org/wiki/CVSS

[5] [5] The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems,
http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf

[6] [6] CVSS Frequently Asked Questions,
http://www.first.org/cvss/faq/#c2

[7] [7] CVSS-SIG Version 2 History,
http://www.first.org/cvss/history.html

[8] [8] Common Vulnerability Scoring System v1 Archive,
http://www.first.org/cvss/v1/