CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosna poboljšanja nove inačice Ubuntu operacijskog sustava

CCERT-PUBDOC-2008-12-250

+CERT.hr u suradnji s LSS

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

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

CARNet CERT, www.cert.hr

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

LS&S, www.LSS.hr

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

Sadržaj

1. Uvod

„Ubuntu“ je kao i svi „Linux” operacijski sustavi besplatan za korištenje. Zasnovan je na „Debian Linux” distribuciji, a proizvodi se pod licencom tvrtke Canonical Ltd. Prednost ovog operacijskog sustava su svakako lakoća i jednostavnost korištenja bilo da se radi o poslovnoj, edukacijskoj ili privatnoj upotrebi. Važno je napomenuti da već nakon same instalacije sustav sadrži sve potrebne programe za obradu i pisanje teksta, tablične proračune, izradu prezentacija, slanje e-mail poruka, obradu fotografija i mnoge druge korisne alate. Važno je napomenuti da je „OpenOffice”, koji je sadržan u samoj instalaciji „Ubuntu“-a, potpuno kompatibilan sa Office paketima drugih proizvođača (Microsoft Office, Word Perfect, KOffice ili StarOffice). Programskim paketima koji su uključeni u „Ubuntu“ korisnicima je omogućena sloboda u izradi, uređivanju i dijeljenju podataka koji su namijenjeni za druge programske pakete ili operativne sustave.

Nova inačica „Ubuntu“ operacijskog sustava se objavljuje svakih 6 mjeseci kako bi se korisnicima omogućila što bolja zaštita i nadogradnja modula vezanih uz rad operacijskog sustava. Kada je u pitanju sama zaštita, bilo zbog propusta ili pojave nove vrste zlonamjernog programskog koda, „Ubuntu“ nudi mogućnost aktualizacije modula sustava putem Interneta.

Operacijski sustav je dobio naziv od riječi afričkog podrijetla *ubuntu* koja u doslovnom prijevodu znači „humanost prema drugima“ ili „ja sam ono što jesam zbog onog tko smo svi mi“.

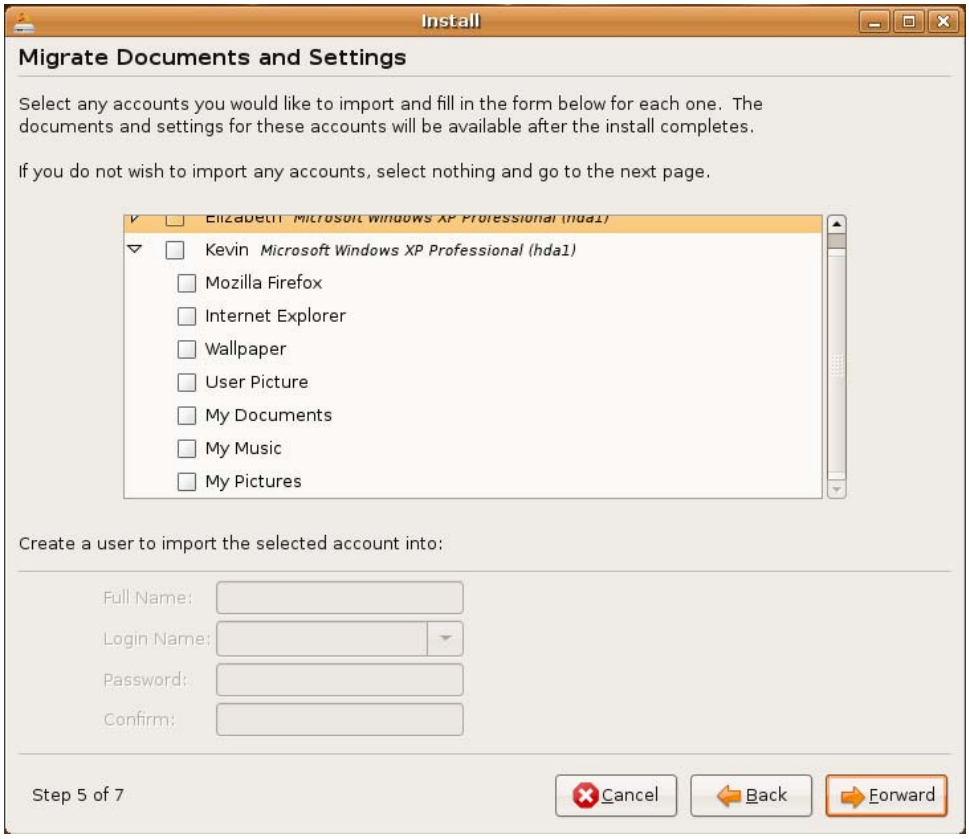
„Ubuntu“ je moguće preuzeti izravno s Interneta ili narudžbom CD medija putem službene stranice. Da bi se pristupilo preuzimanju, na jedan ili drugi način, potrebno je napraviti korisnički račun na službenoj Ubuntu stranici (http://www.ubuntu.com/). Oba načina preuzimanja su potpuno besplatna, te pri narudžbi CD medija nije postavljeno ograničenje na količinu medija koja se naručuje (poštarina je također plaćena). „Ubuntu“ se pojavljuje u nekoliko inačica koje su prilagođene okruženju u kojem će se koristiti: Kubuntu, Edubuntu, Gobuntu, Ubuntu Server Edition i mnoge druge. Kasnije u dokumentu detaljnije su navedene sve inačice „Ubuntu“ operacijskog sustava kao i njihova namjena.

U Hrvatskoj postoji udruga korisnika „Ubuntu“ operacijskog sustava pod imenom Ubuntu-hr. Udruga posjeduje web stranicu (http://www.ubuntu-hr.org/) na kojoj je moguće saznati novosti vezane uz „Ubuntu“ i zatražiti pomoć drugih korisnika. Trenutačno nije moguće preuzeti inačicu „Ubuntu“ operacijskog sustava na hrvatskom jeziku, ali prema vijestima udruge korisnika, hrvatsko sučelje za najnoviju inačicu će biti dostupno vrlo brzo.

U ovom dokumentu napravljen je pregled sigurnosti najnovije inačice „Ubuntu“ operacijskog sustava, 8.10 pod nazivom „Interpid Ibex“. Također će biti navedeni sigurnosni propusti koji su se pojavili u prethodnoj inačici, te koje su zakrpe objavljene u novoj.

2. Što je Ubuntu?

Ubuntu je Linux distribucija koja je prvenstveno namijenjena upotrebi na desktop računalima. Jednostavnost pri upotrebi se pokazala ključnim kriterijem korisnika pri odabiru operacijskog sustava, stoga ne čudi činjenica da je „Ubuntu“ vrlo brzo postao najčešće korišteni Linux operacijski sustav. Počevši od instalacije, koja je brza i prilagođena korisnicima, pa do korištenja i nadogradnje, „Ubuntu“ zadivljuje jednostavnošću. Canonical se obvezao davati podršku korisnicima sustava u vremenskom periodu od 18 mjeseci. Zbog velikog izbora različitih inačica operacijskih sustava (Microsoft Windows, različite inačice Linuxa, itd.) programski paketi koji su sadržani u samoj instalaciji potpuno su kompatibilni sa programskim paketima drugih proizvođača i operacijskim sustavima. Ova mogućnost korisnicima daje potpunu slobodu u razmjeni podataka sa korisnicima drugih operacijskih sustava. Također je moguće, u slučaju prelaska s Windows operacijskog sustava na Ubuntu, preuzeti korisničke podatke i postavke koje su se nalazile u samom operativnom sustavu (My Documents, Favorites, postavke instaliranih programa, itd.)



Slika 1. Prikaz okvira dijaloga pri preuzimanju korisničkih podataka i postavki s drugih operacijskih sustava

„Ubuntu“ u inicijalnoj instalaciji sadrži slijedeće programske pakete i programe:

- OpenOffice - programski paket koji sadrži gotovo sve potrebne programe za obradu i izradu tekstualnih dokumenata („Word Processor“), izradu tabličnih proračuna („Spreadsheet“), te program za izradu prezentacijskih materijala („Presentation“)
- Evolution - program koji sadrži modul za izmjenu e-mail poruka, te modul s kalendarom
- Tomboy - program koji ima namjenu podsjetnika
- Mozilla Firefox - program za pregledavanje sadržaja na Internetu
- F-spot - program za organizaciju, dodavanje i obradu fotografija i slika
- Rythmbox - multimedijski program

Dakako, postoji još cijeli niz programa koje je moguće putem Interneta preuzeti i instalirati na „Ubuntu“. U tzv. „Knjižnici programa“ (eng. *Software library*) se nalazi arhiva u kojoj su programi razvrstani prema namjeni. Svi programi su potpuno besplatni, a preuzimanju se pristupa izravno putem sučelja operacijskog sustava.

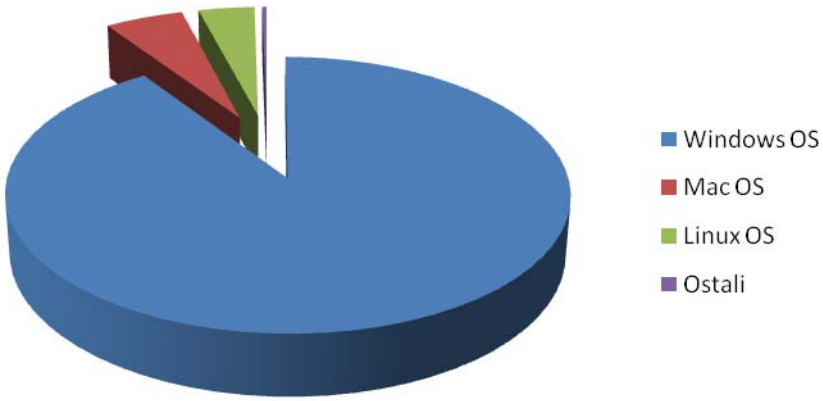
„Ubuntu“ je moguće nabaviti u nekoliko inačica, a svaka je prilagođena okruženju u kojem će se koristiti:

- Ubuntu Desktop - namijenjena upotrebi na osobnim računalima
- Ubuntu Server Edition - inačica koja je namijenjena upotrebi na poslužiteljima (eng. *server*)
- Kubuntu - umjesto GNOME grafičkog sučelja koristi jače i brže KDE grafičko sučelje
- Edubuntu - inačica namijenjena za upotrebu u obrazovnim ustanovama
- Xubuntu - umjesto GNOME grafičkog sučelja koristi XFCE grafičko sučelje koje je namijenjeno slabijim računalima
- Gobuntu - namijenjena desktop računalima uz korištenje isključivo besplatnih programskih paketa
- Ubuntu Mobile Internet Device (MID) Edition - inačica namijenjena upotrebi na novoj vrsti mobilnih računala
- Ubuntu Studio - inačica namijenjena za izradu i izmjenu multimedijskih datoteka
- Mythbuntu - inačica namijenjena za dobivanje efekta kućnog kina na računalu sa programom MythTV

Kao problem pri korištenju operacijskih sustava koji su nastali iz Linuxa, prikazana je podrška za sklopovlje računala. Pošto su drugi operacijski sustavi (Windows i Mac OSX) raširenija i imaju veći broj korisnika, proizvođači sklopovlja u nekim slučajevima ne izrađuju upravljačke programe za operativne sustave temeljene na Linuxu. Međutim, upravljački programi za novije sklopovlje računala se najčešće isporučuju.

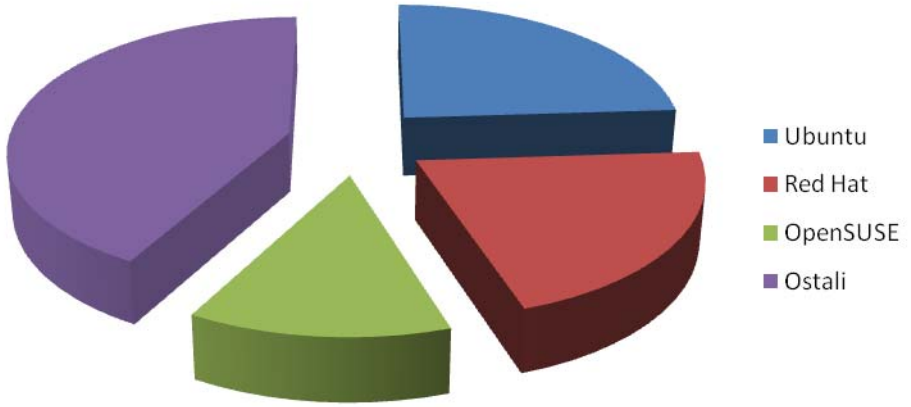
2.1. Statistika

Statistički gledano, Linux distribucije imaju poprilično mali udio korisnika na tržištu. Najveću prednost i dalje imaju Windows operacijski sustavi i prema najnovijim podacima taj udio iznosi 90.6%. Na drugom mjestu po broju korisnika nalaze se Mac operacijski sustavi sa udjelom od 5.3%. Udio Linux distribucija na tržištu iznosi 3.8%.



Slika 2. Prikaz udjela operacijskih sustava na tržištu

Što se tiče udjela na tržištu kod Linux distribucija, prema provedenim anketama i istraživanjima iz početka 2008. godine, Ubuntu svakako ima prednost pred svoja dva najveća konkurenta, Red Hat i Novell OpenSUSE Linuxa. Ubuntu vodi sa udjelom između 23 i 24%, dok je Red Hat distribucija na drugom mjestu sa pripadajućih 21%, a Novell OpenSUSE distribucija bilježi svega 13%.



Slika 3. Prikaz udjela Linux operacijskih sustava (Ubuntu, Red Hat i OpenSUSE)

Za pretpostaviti je da je udio Ubuntu operacijskog sustava porastao za određeni iznos zbog objave nove inačice, „Interpid Ibex". Jedan od razloga naglog širenja Ubuntu distribucije je prilagodba samog operacijskog sustava raznim namjenama.

Što se tiče statistike vezane uz broj propusta, Ubuntu tim redovito izvještava korisnike putem Ubuntu Wiki stranice. Na toj je stranici moguće naći sve informacije vezane uz Ubutnu operacijski sustav. Ubuntu tim na tjednoj osnovi objavljuje web stranicu s novostima (eng. *newsletter*) na kojoj je moguće pronaći informacije poput obavijesti o događanjima vezanim uz Ubuntu, napredak u rješavanju sigurnosnih problema, informacije o prijevodima i razne statistike. Putem Wiki stranice korisnici Ubuntu operacijskog sustava pridonose svojima prijavama sigurnosnih propusta.

Ubuntu tim na web stranici s novostima iznosi broj riješenih i broj novih propusta u sustavu. Propusti su podijeljeni u otvorene, kritične, nepotvrđene, nedodijeljene, te ukupan broj propusta tijekom životnog vijeka svih inačica Ubuntu operacijskog sustava. Podaci su navedeni u **Tabeli 1**. Broj izvan zagrade u pojedinom polju označava trenutačni broj propusta svih inačica Ubuntu operacijskog sustava, a broj u zagradi broj riješenih (označeno minusom ispred broja) ili novootkrivenih propusta (označeno plusom ispred broja).

Tabela 1. Broj sigurnosnih propusta svih inačica Ubuntu operacijskog sustava tijekom zadnjih 6 tjedana

	7.12.-13.12.	**30.11.-06.12.**	**23.11.-29.11.**	**16.11.-22.11.**	**09.11.-15.11.**	**02.11.-08.11.**
Otvoreni	47948 (**-317**)	48265 (**-233**)	48498 (**+42**)	48456 (**-5**)	48461 (**+257**)	48204 (**+264**)
Kritični	15 (**-1**)	16 (**-2**)	18 (**-1**)	19 (**0**)	19 (**0**)	19 (**0**)
Nepotvrđeni	18479 (**-321**)	18800 (**-778**)	19578 (**-97**)	19853 (**-51**)	19904 (**-263**)	20167 (**-218**)
Nedodijeljeni	39822 (**-327**)	40149 (**-197**)	40346 (**+47**)	40299 (**+26**)	40273 (**+261**)	40012 (**+306**)
Svi (životni vijek)	236667 (+1211)	235465 (+1343)	234122 (+1884)	232238 (+1545)	230693 (+1986)	228707 (+2542)

U postocima, vidljiva je promjena u navedenih šest tjedana kod:

- broja otvorenih propusta - smanjenje od 0,53%
- broja kritičnih propusta - smanjenje od 21,05%
- broja nepotvrđenih propusta - smanjenje od 8,37%
- broja nedodijeljenih propusta - smanjenje od 0,47%
- te broja svih propusta tijekom životnog vijeka sustava - povećanje od 3,48%.

Važno je spomenuti da u navedenim periodima nije prijavljen niti jedan kritičan sigurnosni propust.

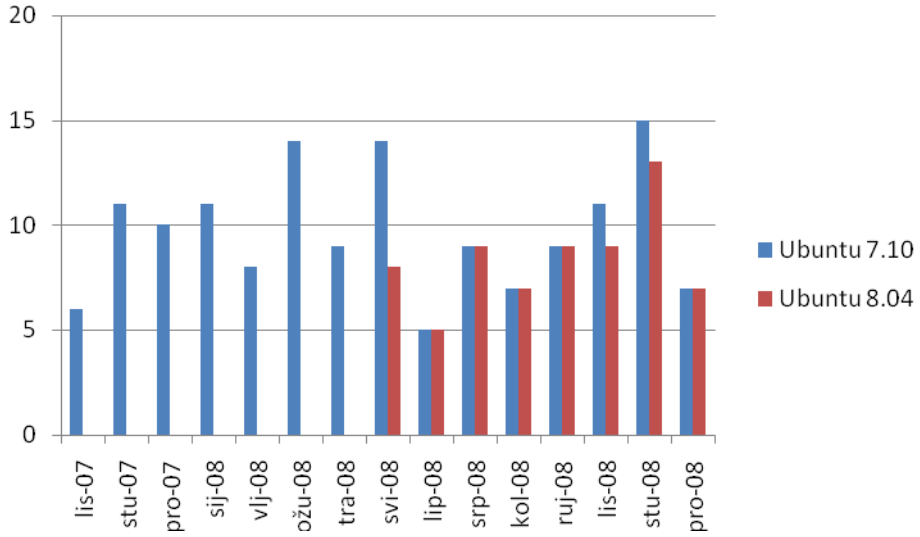
3. Sigurnosni problemi prethodnih inačica

Pri odabiru operacijskog sustava svakako je potrebno razmotriti nekoliko činjenica vezanih uz sustav:

- broj sigurnosnih propusta u životnom vijeku proizvoda,
- kritičnost propusta,
- moguće posljedice i
- brzina kojom se ti propusti rješavaju.

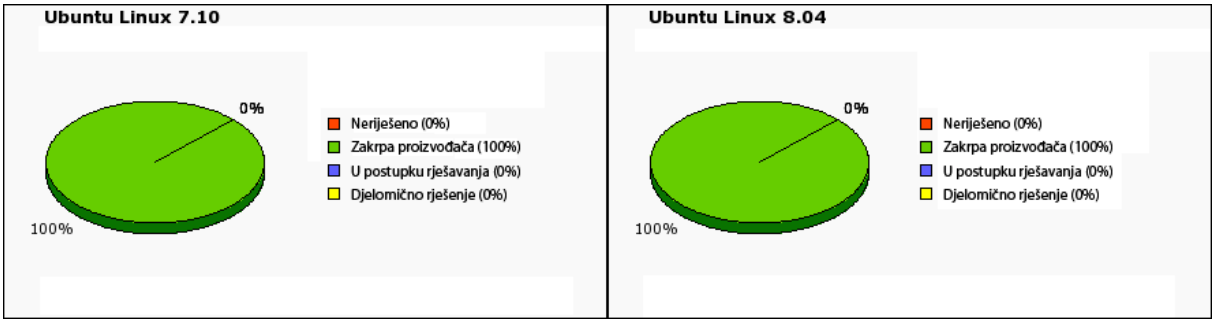
U nastavku će biti navedene karakteristike prethodnih dviju inačica operacijskog sustava Ubuntu. Podaci su preuzeti sa službenih web stranica tvrtke Secunia upravo radi usporedbe sa novom inačicom, „Interpid Ibex".

Ubuntu 7.10, Gutsy Gibbon, objavljen je 18. listopada 2007. godine, a Ubuntu Hardy Heron 24. travnja 2008. godine. Kao i prethodne inačice Ubuntu operacijskog sustava, moguće ih je još uvijek preuzeti sa službenih stranica. Prema statistikama tvrtke Secunia, u operativnom sustavu Ubuntu inačice 7.10 u periodu od 18. listopada 2007. do 15. prosinca 2008. otkriveno je 146 sigurnosnih propusta, a kod inačice 8.04 u periodu od 24. travnja do 15. prosinca 2008. 68 sigurnosnih propusta.



Slika 4. Broj otkrivenih sigurnosnih propusta Ubuntu inačice 7.10 i 8.04

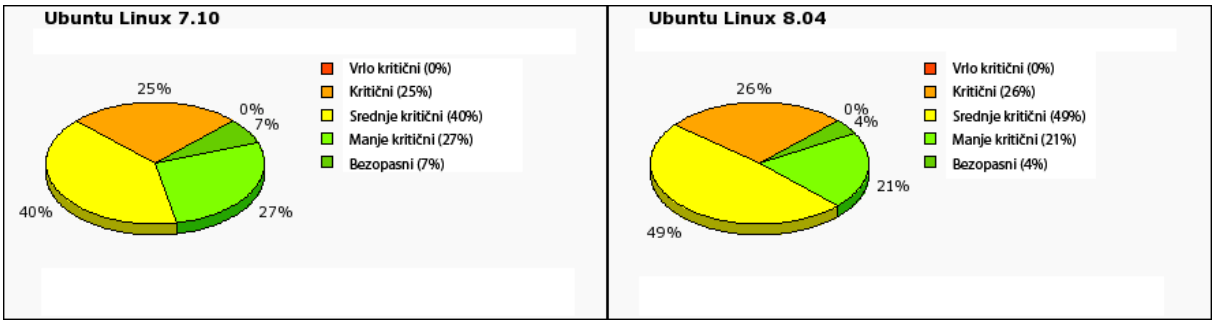
Broj otkrivenih sigurnosnih propusta ove inačice svakako je velik s obzirom na protekli vremenski period od objave. Međutim, treba uzeti u obzir podatak da niti jedan od otkrivenih sigurnosnih propusta nije ostao „otvoren". U nastavku je naveden grafički prikaz broja riješenih sigurnosnih propusta.



Slika 5. Prikaz broja riješenih sigurnosnih propusta

Izvor: Secunia

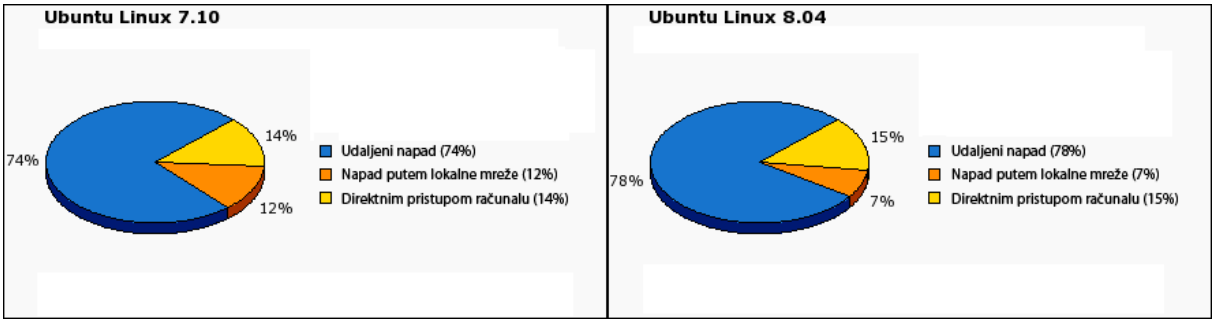
Također je važno spomenuti kritičnost otkrivenih propusta. Podaci su slijedeći:



Slika 6. Prikaz kritičnosti propusta

Izvor: Secunia

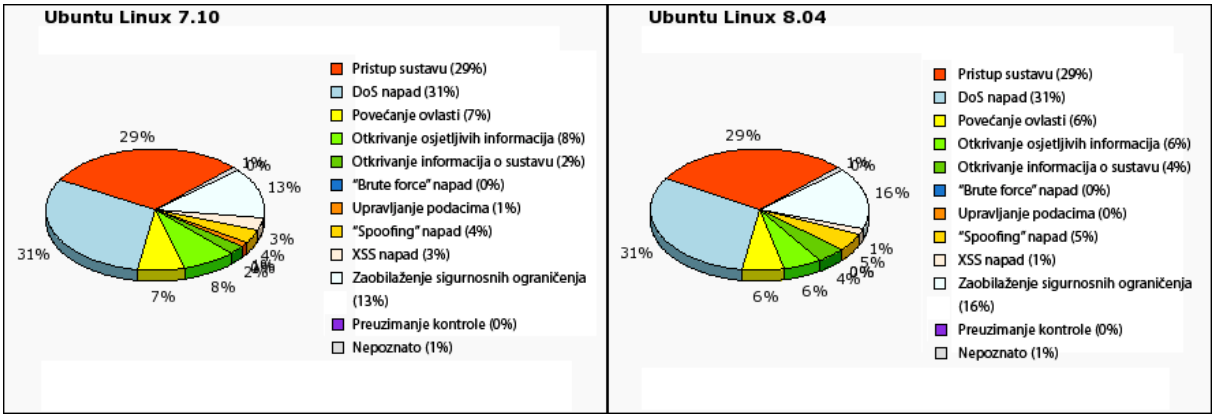
s upućuje na sigurnost sustava, a samim time i na sigurnost podataka i informacija korisnika. Iako operacijski sustavi temeljeni na Linuxu nisu najčešće napadani operacijski sustavi, potrebno je obratiti pažnju na sigurnost podataka na računalu. Korisno je također navesti podatak o vektoru izvršenja napada, tj. mjestu s kojeg je izvršen napad na Ubuntu sustav:



Slika 7. Prikaz vektora izvršavanja napada

Izvor: Secunia

Na slijedećem prikazu moguće je uočiti na koje su vrste napada Ubuntu 7.10 i 8.04 najosjetljiviji, tj. koje su posljedice pronađenih sigurnosnih propusta.



Slika 8. Prikaz posljedica sigurnosnih propusta

Izvor: Secunia

Većina sigurnosnih propusta u ovakvim operacijskim sustavima uzrokovana je instaliranim programima . Isto vrijedi i za Ubuntu operacijski sustav inačica 7.10 i 8.04. Pronađeni sigurnosni propusti u ovim inačicama operacijskog sustava Ubuntu uzrokovani su propustima u instaliranim programima. Tu spadaju oni programi koji su sadržani u samoj instalaciji operacijskog sustava, ali i programi koje je moguće naknadno instalirati. Neki od propusta su:

1. Propusti vezani uz Mozillu Thunderbird:
    - nekoliko ranjivosti uz pomoć kojih napadač može otkriti povjerljive informacije o sustavu, steći višu razinu ovlasti na računalu korisnika ili ugroziti podatke i samo računalo i
    - ranjivost vezana uz poruke e-pošte koje sadrže Javascript kod kojom napadač može pristupiti informacijama u spremniku dolazne e-pošte
2. Propusti vezani uz programski paket OpenOffice:
    - ranjivost vezana uz grešku pri analizi WMF (eng. *Windows Metafile*) datoteka kojom napadač može uzrokovati prepisivanje spremnika (eng. *buffer overflow*) pomoću posebno izrađene StarOffice/StarSuite datoteke i
    - ranjivost vezana uz prepisivanje cijelog broja (eng. *integer overflow*) pri analizi sintakse određenih EMR (eng. *Enhanced Metafile Record*) ili EMF (eng. *Enhanced Metafile*) datoteka pri čemu se može dogoditi prepisivanje spremnika (eng. *buffer overflow*) pomoću posebno izrađene StarOffice/StarSuite datoteke. Uspješno iskorištavanje ove ranjivosti može omogućiti izvršavanje proizvoljnog programskog koda.
3. Propusti vezani uz Mozillu Firefox:
    - ranjivost vezana uz grešku pri analizi datoteka u Mozilli Firefox koje sadrže Javascript kod. Ukoliko korisnik pokrene datoteku napadaču omogućava izvršavanje proizvoljnog programskog koda,
    - razne ranjivosti u mehanizmu za prikaz web stranica koje mogu omogućiti napadaču izvršavanje proizvoljnog programskog koda ili „rušenje“ Mozille Firefox,
    - ranjivost vezana uz pokretač Javascript programskog koda može prouzročiti grešku u memoriji (eng. *memory corruption*) ili izvršavanje proizvoljnog programskog koda i
    - ranjivost vezana uz analizu E4X dokumenata što napadač može iskoristiti za ubacivanje proizvoljnog programskog koda.
4. Propusti vezani uz Libxml2 - program za analizu XML dokumenata
5. Propusti vezani uz Moodle CMS sustav:
    - ranjivosti vezane uz PHP kod kojima napadač može ubaciti i izvršiti proizvoljni programski kod
6. Propusti vezani uz Xine - multimedijski program:
    - ranjivost vezana uz analizu MPEG (eng. *Motion Picture Expert Graphics*) datoteka koju se može iskoristiti za prepisivanje spremnika, te izvršavanje proizvoljnog programskog koda uz pomoć posebno izrađene MPEG datoteke

Ovo su neki od propusta koji su označeni kao kritični, međutim nije navedena cijela lista. Također, postoje sigurnosni propusti u samom operativnom sustavu, no nisu označeni kao kritični i ranjivosti su riješene u vrlo kratkom roku. Kao što je vidljivo iz prikaza na **Slici 4.**, svi prijavljeni sigurnosni propusti inačica 7.10 i 8.04 su riješeni.

4. Sigurnost Ubuntu 8.10 - „Interpid Ibex“ inačice

Kod svih operacijskih sustava je potrebno posvetiti pažnju na zaštitu računala, pa tako i kod Ubuntu Linux operacijskog sustava. Iako je Ubuntu nakon same instalacije potpuno zaštićen, velik broj korisnika na sami operacijski sustav instalira mnogo programa čime se povećava mogućnost pojave propusta. Velik broj korisnika po instalaciji mijenja početne zaštitne postavke u modulu Ubuntu operacijskog sustava. Ubuntu knjižnica programa sadrži velik broj programa za zaštitu i sigurnost računala i dostupni su korisnicima za preuzimanje. Na Ubuntu Wiki stranici su stavljene preporuke korisnicima koje su najbolje postavke za optimalnu sigurnost računala, te koje je programe i alate poželjno koristiti u tu svrhu. Neke od važnijih dane su u nastavku:

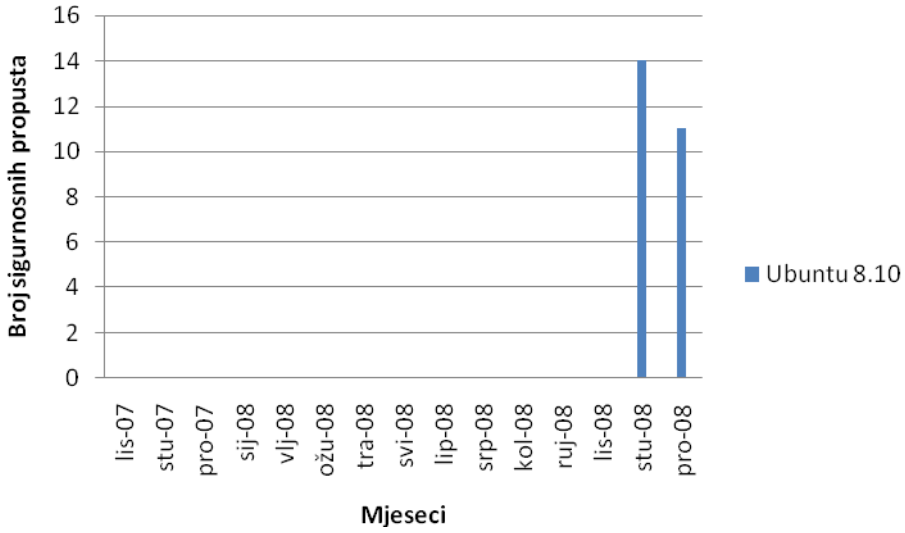
1. Automatska aktualizacija (eng. Automatic Update) operacijskog sustava
    - u početnim je postavkama namješteno da čim se pojavi zakrpa ili nova funkcija za operacijski sustav ili neki od instaliranih programa, korisniku se pojavi obavijest. Međutim, moguće je unosom određenog programskog koda podesiti sustav da bez ikakvih obavijesti instalira novitete.
2. Zaštita sustava jakom lozinkom
    - u samom operativnom sustavu se nalazi program APG (eng. *Automated Password Generator*) kojim je moguće stvoriti lozinku koju je gotovo nemoguće probiti. Program na zahtjev korisnika stvara šifre za razne namjene kao što su lozinke za račune e-pošte, pristup računalu, itd.
3. Instalacija sigurnosnih alata
    - Wireshark (prije Ethereal) - popularni program kojem je namjena analiza mrežnog prometa
    - Nessus - program koji se koristi za pregledavanje zadanih računala i mreža u potrazi za sigurnosnim propustima, te izvještava korisnika o pronađenim propustima
    - Etherape - program koji prikazuje mrežnu aktivnost
    - Chkrootkit - namjena mu je otkrivanje da li je računalo ugroženo nekim od napada
    - Tiger - program koji pronalazi sigurnosne probleme u UNIX operacijskom sustavu i javlja korisniku ukoliko je sigurnost sustava ili podataka ugrožena
    - Denyhosts - program koji pretražuje sustav kako bi pronašao tragove „brute force“ napada i potom blokira IP (eng. *Internet Protocol*) adrese s kojih su izvršeni
4. Instalacija vatrozida (eng. *firewall*)
    - Firestarter - jedan od vatrozida koje Canonical preporučuje
    - Fwknop - program koji omogućuje administratorima sustava ograničavanje pristupa mrežnim podacima i onima na serveru na način da identificira korisnike prije nego što im dopusti bilo slanje ili primanje TCP/IP (eng. *Transmission Control Protocol/Internet Protocol*) paketa
5. Program za poboljšanje sigurnosti sustava
    - Bastille Linux - interaktivni alat za poboljšanje sigurnosti sustava i smanjenje osjetljivosti na napade. Korisnik odabire razinu zaštite odabirom mogućnosti koje program nudi (spam zaštita, zaštita korisničkih računa, zaštita od izvršavanja zlonamjernih programskih kodova, itd.). Ne preporučuje se početnicima jer je postavljanje samog alata vrlo složeno.
6. Instalacija programa za provjeru ispravnosti sustava
    - BitDefender Linux Edition - pretražuje sustav radi pronalaska zlonamjernih programskih kodova i čišćenje istih
    - FileIntegrityAIDE - pretražuje sistemske datoteke radi otkrivanja neovlaštenih izmjena od strane napadača
7. Razni programi za sigurno brisanje podataka
    - Coreutils
    - Wipe
    - Secure-Delete

8. Zaštita sistemskih datoteka i datoteka korisnika
    - TrueCrypt - program koji korisniku omogućuje stvaranje skrivenog prostora na disku i na taj način zaštitu povjerljivih ili osobnih datoteka
    - eCryptfs - program koji korisniku omogućava zaključavanje datoteka lozinkom
9. Programi za zaštitu e-pošte
    - PGP (eng. Pretty Good Privacy) - program koji omogućuje korisniku zaštitu i identifikaciju pri slanju ili primanju e-pošte
10. Instalacija antivirusnog programa
    - Linuxvirus
    - AVG Antivirus
    - Panda Antivirus
    - BitDefender Antivirus
    - ClamAV
11. Alati koji korisniku omogućuju anonimnost pri korištenju Interneta
    - The Onion Router - skup alata koji poboljšava sigurnost korisnika pružajući anonimnost pri pregledavanju Interneta, dopisivanja putem IM (eng. Instant Messaging) programa, IRC (eng. Internet Relay Chat) razgovora, te drugim programima koji komuniciraju putem TCP protokola

4.1. Statistika

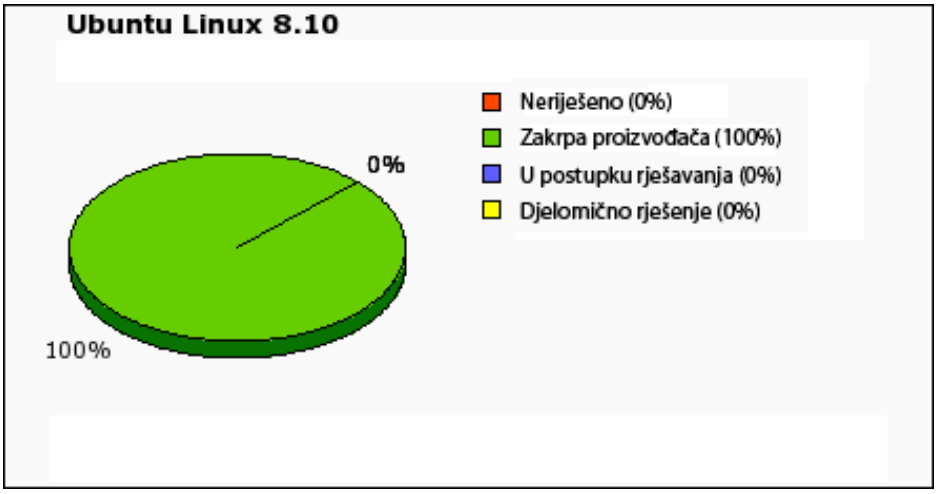
U protekla dva mjeseca, od objave nove inačice, prijavljeno je 25 sigurnosnih propusta koji mogu utjecati na sigurnost računala korisnika. Neki od ovdje uračunatih propusta utjecali su na sve inačice operacijskog sustava Ubuntu.

U nastavku je prikazan grafički prikaz broja propusta po mjesecima:



Slika 9. Prikaz broja sigurnosnih propusta Ubuntu 8.10

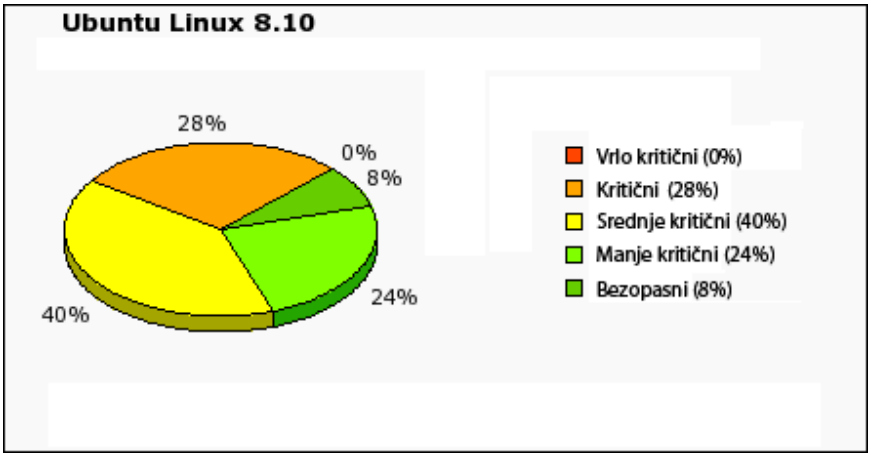
Važno je također navesti trenutno stanje propusta, tj. da li su svi propusti riješeni ili neki od propusta još uvijek ugrožavaju korisnike. Kako se vidi u nastavku, Canonical i Ubuntu zajednica su ostali dosljedni prijašnjim rezultatima, pronađeni su propusti riješeni u što kraćem vremenskom roku.



Slika 10. Prikaz broja riješenih zakrpa u Ubuntu 8.10

Izvor: Secunia

Vrlo važna stvar vezana uz sigurnosne propuste je i na koji način, ali i u kojoj mjeri mogu ugroziti računalo korisnika. U nastavku je naveden grafički prikaz kritičnosti sigurnosnih propusta podijeljen u pet skupina: vrlo kritični, kritični, srednje kritični, manje kritični i bezopasni.

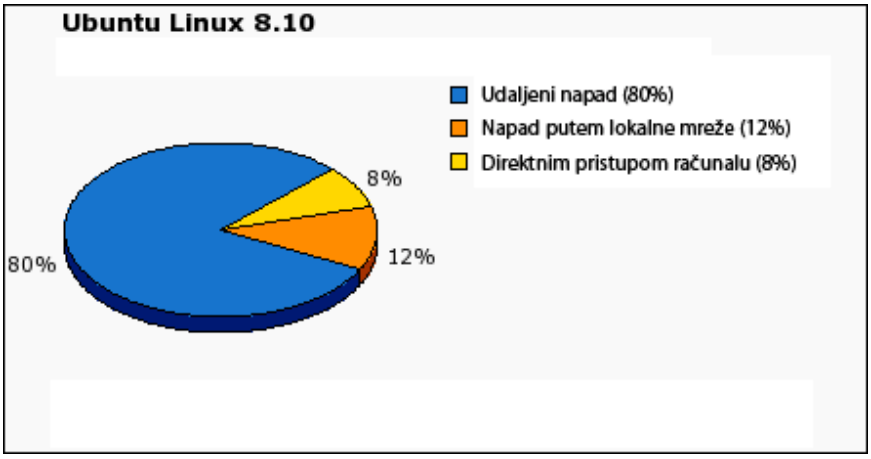


Slika 11. Prikaz kritičnosti sigurnosnih propusta Ubuntu 8.10

Izvor: Secunia

Ubuntu inačica 8.10 najčešće je napadana udaljenim napadima (eng. *remote attack*). Čak 80% prijavljenih napada izvršeno je udaljenim napadom, što govori da je ipak potrebno obratiti pažnju na sigurnost Ubuntu sustava. Na temelju ovih podataka moguće je zaključiti više o sigurnosnim propustima koji će biti navedeni u nastavku dokumenta.

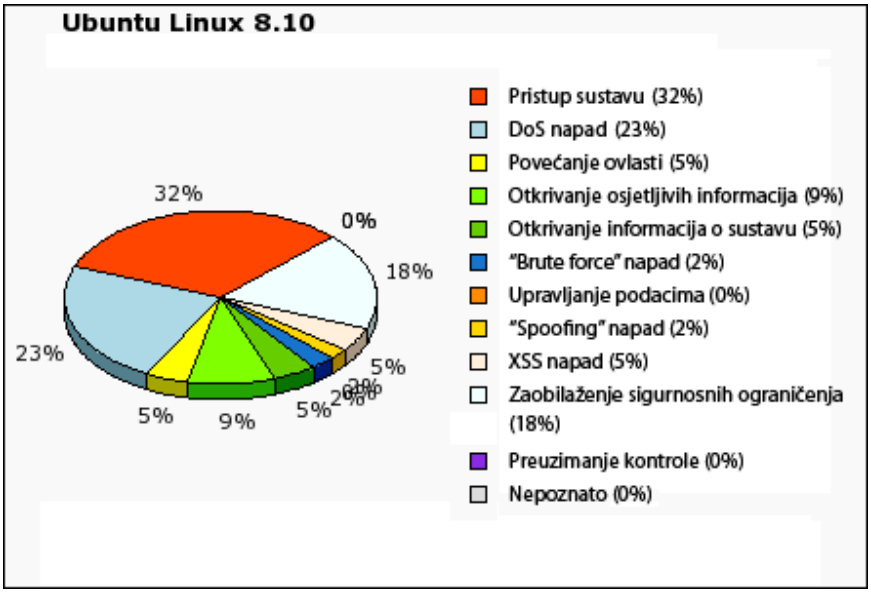
U nastavku je naveden grafički prikaz vezan uz vektor izvršenja napada:



Slika 12. Prikaz vektora izvršenja napada na Ubuntu 8.10

Izvor: Secunia

Kao što će u nastavku biti prikazano, vidljivo je da su propusti u operacijskom sustavu Ubuntu 8.10 omogućili napadačima direktan pristup sustavu u 32% napada, DoS (eng. *Denial of Service*) napad je izvršen u 23% slučajeva, a kao treća posljedica s udjelom od 18% navedeno je zaobilaženje sigurnosnih ograničenja.



Slika 13. Prikaz posljedica sigurnosnih propusta

Izvor: Secunia

4.2. Sigurnosni propusti

Iako je ova inačica relativno nova, otkriveni su sigurnosni propusti koji mogu ugroziti korisnika ukoliko se operacijski sustav ne aktualizira redovito. Kao što je zamijećeno u prethodnim inačicama Ubuntu operacijskog sustava, napadač može:

- steći ovlast nad računalom
- ukrasti podatke
- onesposobiti samo računalo korisnika.

Veći dio sigurnosnih propusta ugrožavao je korisnike svih inačica Ubuntu operacijskog sustava, no također su pronađeni neki specifični za inačicu Ubuntu 8.10. Svi dosad otkriveni propusti u ovoj inačici su uspješno riješeni. Neki od propusta specifičnih za ovu inačicu su navedeni u nastavku.

1. Propust u alatu libvirt - alatu za interakciju sa virtualnim sučeljem Linux operacijskih sustava
   - pomoću ovog propusta napadač je mogao steći ograničena prava administratora. Propust je uočen u inačicama od 0.3.2 do 0.5.1, no postoji mogućnost da je utjecao i na ostale inačice.
2. Propust u programu Little CMS - programu za upravljanje bojama u operativnom sustavu
   - pomoću posebno izrađene JPG/JPEG (eng. *Joint Photographic Experts Group*) datoteke bilo je moguće uzrokovati grešku u radu programa i prepisivanje spremnika. Ovaj propust je utjecao na inačice programa prije 1.15. Zloupotrebom ovog propusta napadač je mogao izvršiti zlonamjerni programski kod.
3. Propust u programu Vinagre - VNC (eng. *Virtual Network Computing*) klijent za operativne sustave sa GNOME sučeljem
   - propust uzrokovan greškom u zapisu u funkciji *src/vinagre-utils.c*. Propust je bilo moguće iskoristiti na način da se korisnika prijevarom uvjeri da otvori posebno izrađenu .vnc datoteku ili spajanjem na zlonamjernog VNC poslužitelja. Zloupotrebom ovog propusta napadač je mogao izvršiti zlonamjerni programski kod.
4. Propust u programu Compiz Fusion - programu za grafičko korisničko sučelje
   - propust u dodatku Expo koji je mogao omogućiti napadaču pristup zaključanom računalu.
5. Propust u programu AWStats - programu za prikupljanje statističkih podataka u mrežnom sustavu ili na Internetu
   - ukoliko je korisnik posjetio zlonamjernu web stranicu, napadač je mogao izvršiti zlonamjerni HTML (eng. *HyperText Markup Language*) kod u korisnikovom pregledniku.
6. Propust u SNMP (eng. *Simple Network Management Protocol*) protokolu koji služi za nadgledanje stanja mrežne računalne opreme
   - napadač je mogao uzrokovati prepisivanje spremnika te izvršiti DoS napad
7. Propust u programu ClamAV - antivirusnom programu za Linux operativne sustave
   - zbog greške u funkciji *libclamav/special.c* paketa bilo je moguće pomoću posebno izrađene JPEG datoteke uzrokovati prepisivanje spremnika ili „rušenje“ programa
8. Propusti u jezgri (eng. *kernel*) operacijskog sustava
   - propust u USBLCD pokretačkom programu kod kojeg sustav ne ograničava količinu potrebne memorije za zapisivanje podataka na tvrde diskove što je moglo uzrokovati „rušenje“ sustava.
   - propusti u funkcijama sustava kojima se mogao izvršiti DoS napad, steći višu razinu ovlasti na sustavu, te izvršiti zlonamjerni programski kod.
9. Propusti u programu Samba - program za dijeljenje datoteka i mrežnih pisača kompatibilan s Windows operacijskim sustavima
   - napadač je mogao steći ovlasti na računalu i doći do povjerljivih informacija
10. Propust u GnuTLS alatu - alat koji sadrži skup protokola za sigurnu mrežnu komunikaciju
    - propust je uzrokovan greškom pri potvrdi X.509 certifikata i moglo ga se iskoristiti za izvršavanje MITM (eng. *Man-in-the-middle*) napada.
11. Propust u Dovecot poslužitelju - program za stvaranje IMAP (eng. *Internet Message Access Protocol*) i POP3 (eng. *Post Office Protocol version 3*) poslužitelja namijenjen za operativne sustave koji se temelje na Linuxu/Unixu
    - javljanje greške pri analizi zaglavlja e-poruke, što napadač može iskoristiti na način da zabrani korisniku pristup spremniku e-pošte posebno izrađenim zaglavljem e-poruke. Napadač potom može izvršiti DoS napad.

5. Usporedba sa drugim operacijskim sustavima

Radi što boljeg prikaza funkcionalnosti i sigurnosti Ubuntu operacijskog sustava u nastavku će biti navedeni statistički podaci vezani uz sigurnost drugih konkurentnih operacijskih sustava. Za primjer će biti uzeta Microsoft Windows Vista koja je ulaskom na tržište osvojila značajan broj korisnika. Nadalje, biti će prikazani statistički podaci drugih operacijskih sustava temeljenihh na Linux/Unix jezgri, za koje se tvrdi da su velika konkurencija Ubuntu operativnom sustavu, poput openSUSE inačice 11.0, te Fedore inačice 9.0.

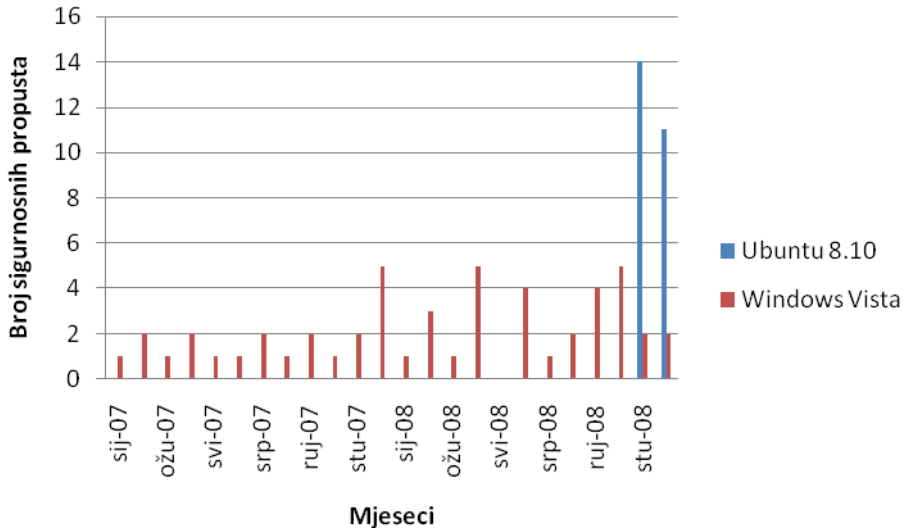
Tabela 2. Broj sigurnosnih propusta operacijskih sustava tijekom životnog vijeka proizvoda

	Ubuntu 8.10	Windows Vista	openSUSE 11.0	Fedora 9.0
Vrlo kritični	0 (0%)	1 (2%)	0 (0%)	0 (0%)
Kritični	7 (27%)	17 (33%)	12 (36%)	26 (16%)
Srednje kritični	10 (38%)	9 (18%)	13 (39%)	62 (39%)
Manje kritični	7 (27%)	19 (37%)	7 (21%)	59 (37%)
Bezopasni	1 (8%)	5 (10%)	1 (3%)	13 (8%)

5.1. Usporedba Ubuntu 8.10 i Windows Vista

Windows Vista je operacijski sustav na kojem je Microsoft radio duže od očekivanog. Najave revolucionarnih novih alata, mogućnosti i postavki svakako su pobudile zanimanje korisnika. Korisnici su vrlo brzo prihvatili novosti, te se prilagodili promjenama.

Vrijedi spomenuti da je u Windows Vista operativnom sustavu u životnom vijeku pronađen relativno malen broj sigurnosnih propusta kojima su napadači mogli ugroziti korisnike. U periodu od gotovo dvije godine pronađen je 51 sigurnosni propust.



Slika 14. Prikaz broja sigurnosnih propusta operacijskih sustava Windows Vista i Ubuntu 8.10

Kada su u pitanju sigurnosni propusti u Windows Vista operativnom sustavu, čak 6 (12%, kod Ubuntu 8.10 0%) propusta još uvijek nije „zakrpano“, za 44 (86%, kod Ubuntu 8.10 100%) propusta Microsoft je objavio zakrpu, a 1 (2%, kod Ubuntu 8.10 0%) propust je u postupku rješavanja. Računala na kojima je postavljen Windows Vista operacijski sustav su najčešće ugrožena udaljenim napadima, čak u 55% (što je 25% manje nego kod Ubuntu 8.10) prijavljenih slučajeva. Posljedice napada su najčešće bile:

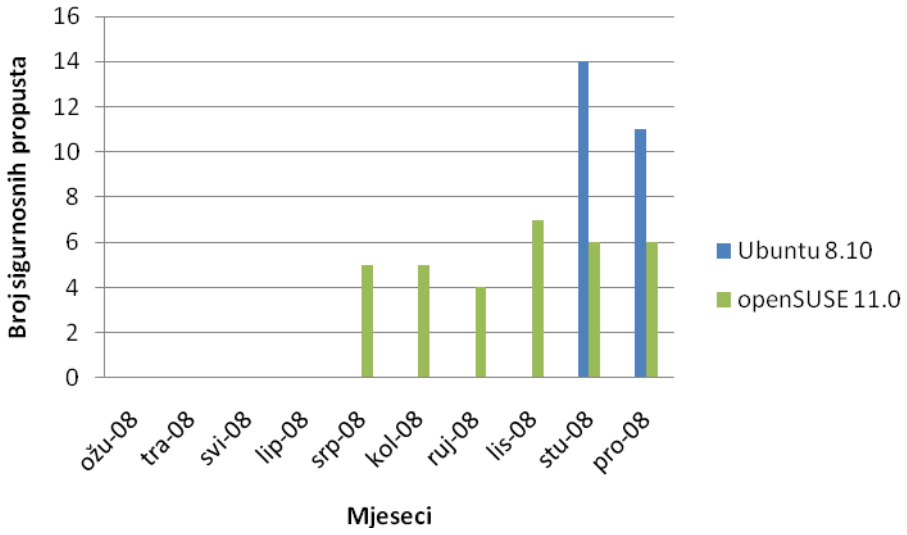
- pristup sustavu - 41% slučajeva (9% više nego kod Ubuntu 8.10)
- DoS napad - 17% slučajeva (6% manje nego kod Ubuntu 8.10)
- povećanje razine ovlasti - 17% slučajeva (12% više nego kod Ubuntu 8.10)

- te otkrivanje osjetljivih informacija - 11% slučajeva (2% više nego kod Ubuntu 8.10).

5.2. Usporedba Ubuntu 8.10 i openSUSE 11.0

OpenSUSE inačica 11.0 operacijski sustav koji se temelji na Linuxu i objavljena je u srpnju 2008. godine, a prema najavama proizvođača, tvrtke Novell, trebala bi dostići konkurenciju. U novoj inačici pojavio se velik broj novosti u samoj jezgri operacijskog sustava, grafičkom sučelju, ali i poboljšanje u radu sustava.

Od objave u lipnju, pa do 15. prosinca pronađena su 33 sigurnosna propusta u operativnom sustavu. Prema izvoru Secunia, u openSUSE 11.0 operativnom sustavu nije pronađen niti jedan vrlo kritičan propust, no pronađeno je 12 kritičnih (5 propusta više nego kod Ubuntu 8.10), 13 srednje kritičnih (3 propusta više nego kod Ubuntu 8.10), 7 manje kritičnih (jednako kao i kod Ubuntu 8.10) te jedan propust koji ne predstavlja opasnost (jednako kao i kod Ubuntu 8.10).



Slika 15. Prikaz broja sigurnosnih propusta operacijskih sustava openSUSE 11.0 i Ubuntu 8.10

Svi propusti koji su prijavljeni su također i ispravljeni. Čak 76% računala na kojima je postavljen openSUSE 11.0 operacijski sustav napadači su ugrozili udaljenim napadima (što je 4% manje nego kod Ubuntu 8.10), 12% napada je izvršeno putem lokalne mreže (jednako kao i kod Ubuntu 8.10) i 12% izravnim pristupom računalu (što je 4% više nego kod Ubuntu 8.10). Posljedice napada su najčešće bile:

- pristup sustavu - 19% slučajeva (13% manje nego kod Ubuntu 8.10)
- DoS napad - 24% slučajeva (1% više nego kod Ubuntu 8.10)
- zaobilaženje sigurnosnih ograničenja - 15% slučajeva (3% manje nego kod Ubuntu 8.10)
- te otkrivanje osjetljivih informacija - 12% slučajeva (3% više nego kod Ubuntu 8.10).

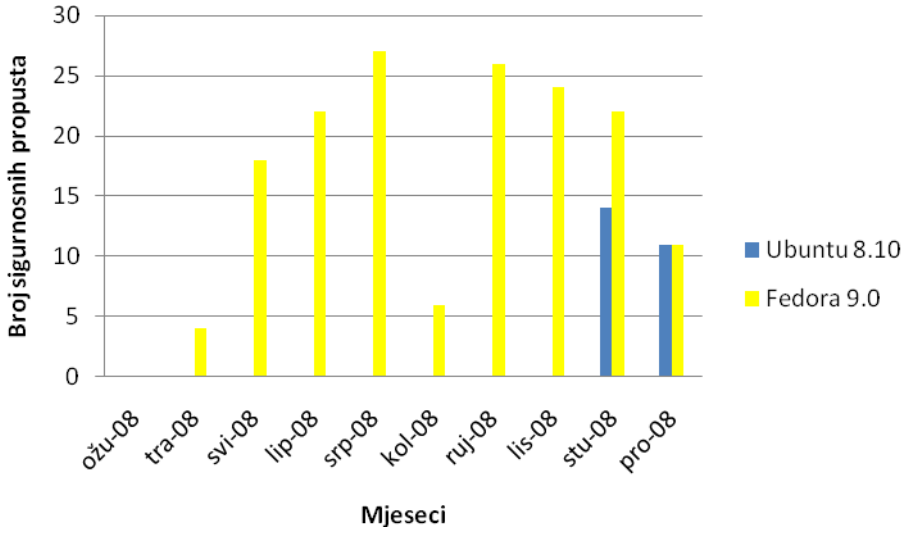
5.3. Usporedba Ubuntu 8.10 i Fedora 9

Fedora je još jedna od brojnih Linux distribucija, a razvoj ovog operacijskog sustava sponzorira tvrtka RedHat. U Fedoru 9 je ugrađeno KDE (eng. *K Desktop Environment*) desktop okruženje s mnoštvom noviteta, najnovija inačica Linux jezgre i nova inačica GNOME grafičkog sučelja. Fedora 9 je objavljena u travnju 2008. godine, a prije nekoliko dana i slijedeća generacija - Fedora 10.

Fedora 9 je među odabranim kandidatima imala najveći broj propusta u relativno kratkom vremenskom periodu. Tvrtka Secunia je objavila čak 160 sigurnosnih propusta, od kojih:

- niti jedan vrlo kritičan (jednako kao i kod Ubuntu 8.10)
- 26 kritičnih propusta (što je 19 propusta više nego kod Ubuntu 8.10)
- 62 srednje kritična propusta (što je 52 propusta više nego kod Ubuntu 8.10)
- 59 manje kritičnih propusta (što je 52 propusta više nego kod Ubuntu 8.10)
- te 13 bezopasnih propusta (što je 12 propusta više nego kod Ubuntu 8.10).

U nastavku je uspoređen broj propusta Fedora 9 i Ubuntu 8.10 operacijskih sustava.



Slika 16. Prikaz broja sigurnosnih propusta operacijskih sustava Fedora 9 i Ubuntu 8.10

Svi propusti pronađeni u Fedora 9 operativnom sustavu su ispravljeni. Veliki broj propusta je zasigurno jedan od razloga zbog kojeg je ovaj nekada vrlo popularni operacijski sustav počeo gubiti korisnike. Računala na kojima je instaliran Fedora 9 operacijski sustavi najčešće su ugrožavana udaljenim napadima i to u 78% slučajeva (što je 2% manje nego kod Ubuntu 8.10), putem lokalne mreže u 10% slučajeva (što je 2% manje nego kod Ubuntu 8.10) i izravnim pristupom u 12% slučajeva (što je 4% više nego kod Ubuntu 8.10). Neke od posljedica ovih napada su:

- pristup sustavu - 24% slučajeva (8% manje nego kod Ubuntu 8.10)
- DoS napad - 26% slučajeva (3% više nego kod Ubuntu 8.10)
- zaobilaženje sigurnosnih ograničenja - 12% slučajeva (6% manje nego kod Ubuntu 8.10)
- te XSS napad - 10% slučajeva (5% više nego kod Ubuntu 8.10).

6. Zaključak

Ubuntu je Linux operacijski sustav prilagođen svim korisnicima. Korisnik odabirom ovog operacijskog sustava dobiva niz korisnih i funkcionalnih programa, ali i primjerenu zaštitu računala i podataka. Problemi sa kompatibilnosti koje drugi operacijski sustavi, temeljeni na Linuxu, imaju sa Windows ili Mac operacijskim sustavima su u ovom primjeru riješeni. Svaka je komponenta ovog sustava prilagođena izmjeni podataka i dokumenata s korisnicima drugih inačica operacijskih sustava. Korisnicima je također na raspolaganju velik izbor besplatnih programa raznih namjena uz pomoć kojih je moguće Ubuntu operativnom sustavu pridodati neke dodatne funkcionalnosti.

Kao što je vidljivo iz prije navedenih podataka, Ubuntu se redovito održava i opasnost od gubitka podataka je minimalna. Na Ubuntu projektu sudjeluje tim stručnjaka, ali i velika zajednica „običnih" korisnika, čime se svakim danom povećava vrijednost i kvaliteta ovog operacijskog sustava otvorenog koda. Pravovremenom reakcijom uspješno su otklonjeni svi sigurnosni propusti koji su dovodili u pitanje sigurnost korisnika i njihovih računala.

Usprkos uspješnosti u rješavanju problema sa propustima, potrebno je primjereno zaštititi sustav programima poput vatrozida, antivirusnog programa, te drugih alata koji mogu poslužiti u svrhu zaštite. Preporuka korisnicima računala je da svakako isprobaju ovaj besplatni operacijski sustav.

7. Reference

[1] Ubuntu operacijski sustav, http://www.ubuntu.com/, prosinac 2008.

[2] Opis Ubuntu operacijskog sustava, http://www.ubuntu.com/products/whatisubuntu, prosinac 2008.

[3] Udruga „Ubuntu“ korisnika u Hrvatskoj, http://www.ubuntu-hr.org/, listopad 2008.

[4] Ubuntu, http://hr.wikipedia.org/wiki/Ubuntu#Ina.C4.8Dice, studeni 2008.

[5] Ubuntu Wiki, https://wiki.ubuntu.com/, prosinac 2008.

[6] Vijesti vezane uz Ubuntu, https://wiki.ubuntu.com/UbuntuWeeklyNewsletter/Issue121, prosinac 2008.

[7] Secunia - Ubuntu 7.10, http://secunia.com/advisories/product/16251/?task=statistics, prosinac 2008.

[8] Secunia - Ubuntu 8.04, http://secunia.com/advisories/product/18611/?task=statistics, prosinac 2008.

[9] APG, http://www.adel.nursat.kz/apg/, prosinac 2008.

[10] Ubuntu Wiki sigurnost, https://help.ubuntu.com/community/Security, prosinac 2008.

[11] Secunia - Ubuntu 8.04, http://secunia.com/advisories/product/20299/?task=statistics, prosinac 2008.

[12] Secunia - Winows Vista, http://secunia.com/advisories/product/13223/, prosinac 2008.

[13] Secunia - openSUSE 11.0, http://secunia.com/advisories/product/19180/, prosinac 2008.

[14] Secunia - Fedora 9, http://secunia.com/advisories/product/18642/, prosinac 2008.

[15] Fedora Project, http://fedoraproject.org/, prosinac 2008.

[16] openSUSE 11.0, http://www.opensuse.org/en/, prosinac 2008.