Analýza slabin zveřejněných v roce 2011

Analýza slabin v operačních systémech a prohlížečích

~~Zero-day~~ Zero years attack

Leden 2012

Pohled tvůrce analýzy na slabiny v počítačových programech

Slabiny v operačních systémech nebo aplikačních programech byly, jsou a pravděpodobně i budou. To je realita IT světa.

V tomto dokumentu jsou zhodnoceny slabiny, které v operačních systémech nebo prohlížečích byly zveřejněny a opraveny v roce 2011.

Hodnocení slabin a určení jejich závažnosti jsme nechali na jiné týmy. Především z MITRE, NIST a dalších týmů, které se zabývají shromažďováním informací a testováním závažnosti konkrétních slabin.

Původní analýza chyb za rok 2010 a její letošní pokračování jsou zaměřeny na hledání vysvětlení úspěšných útoků na relativně dobře zabezpečené osobní počítače, případně firemní počítačové sítě.

V každém programu se objevují méně či více kritické slabiny. Již v analýze slabin zveřejněných v roce 2010 jsme zjistili, že se objevují slabiny, které jsou v několika po sobě jdoucích verzích konkrétního programu.

Pro vytvoření škodlivého programu, který zasáhne větší komunitu uživatelů je třeba nejprve objevit novou vážnou slabinu v počítačovém programu. Dále je třeba takovou slabinu otestovat, vytvořit škodlivý program a zajistit umístění takového škodlivého programu na počítače obětí. Uvedený postup vyžaduje velké zkušenosti a současně čas na přípravu škodlivého kódu. Proto je vedle závažnosti slabiny velmi důležitá i délka po kterou byla slabina přístupná a bylo jí možné zneužít.

Extrémně kritická slabina si vždy zasluhuje pozornost. Pokud byla slabina v konkrétním programu několik týdnů, je riziko jejího zneužití výrazně nižší než v případě jiné kritické slabiny, která byla v programech několik let. Jednoduše proto, že i ten nejlepší hacker nedokáže během několika týdnů objevit novou slabinu a nestihne vytvořit virus, který by novou slabinu zneužíval.

V průběhu analýzy jsme našli velké rozdíly v době, po jakou byly zveřejněné slabiny v konkrétních programech. Zjištěná doba existence slabiny v programu se pohybuje od dvou měsíců u jednoho prohlížeče až po 11 (jedenáct) let u jiného.

Tato analýza chce přispět k vysvětlení příčin, jak mohly některé viry proniknout a působit v jednotlivých počítačích nebo celých informačních systémem mnoho měsíců aniž by byly odhaleny.

Analýza operačního systémy Windows a prohlížečů

Obsah analýzy

1 Výsledky analýzy

1.1 Operační systém Windows

V roce 2011 bylo v operačním systému Windows zveřejněno **96** slabin. Přičemž celkem **83** slabin bylo společných i pro verze Windows VISTA a XP. Celkem **83** slabin zveřejněných v roce 2011 bylo v operačním systému Windows více jak **3500 dnů**[1] než byly tyto slabiny zveřejněny a opraveny.

1.2 Prohlížeče

Microsoft Internet Explorer 9.0

V případě prohlížeče Microsoft (Windows) Internet Explorer 9 jsme v průběhu analýzy zjistili celkem **31** (třicet jedna) slabin v poslední verzi prohlížeče, z čehož **28** (dvacet osm) slabin bylo kritických. Velmi alarmující je zjištění, že **28** (dvacet osm) slabin, které byly zveřejněné v roce 2011 a **48** slabin objevených v roce 2010 bylo v prohlížeči MSIE více jak **3500 dnů** aniž by tyto slabiny někdo zveřejnil a opravil.

Google Chrome 16

V případě prohlížeče Google Chrome, konkrétně v jeho verzi číslo 16 jsme v průběhu analýzy nezjistil slabinu. V průběhu roku 2011 bylo zveřejněno celkem **398** slabin v různých starších verzích prohlížeče Google Chrome. Žádná zjištěná slabina nebyla společná pro dvě verze prohlížeče Google Chrome.

V případě Google Chrome jsme nezjistili slabinu společnou se staršími verzemi prohlížeče Chrome. Maximální doba existence slabiny zveřejněné v roce 2011 byla **63 dnů.**

Mozila Firefox 9.0 a 8.0

V případě prohlížeče Mozilla Firefox verze 8.0 jsme v průběhu analýzy zjistil celkem **11** slabin, přičemž všech **11** slabin bylo kritických. Všech 11 slabin bylo společných s verzí Firefox 3.6. To znamená, že případný útočník měl dva roky, zhruba **700 dnů** na odhalení a zneužití slabiny společné pro verzi 8 a 3.6.

V případě verze 9 bylo zveřejněno **6** (šest) slabin. Všech **6** (šest) slabin bylo kritických. Žádná ze zveřejněných slabin nebyla společná s žádnou z předchozích verzích prohlížeče Firefox. Tyto chyby byly v prohlížeči necelý měsíc, tedy méně než **30 dnů**.

1 Vysvětlení výpočtu dnů kdy existovala konkrétní slabina je uvedeno v kapitole číslo 2.

2 Počet dnů kdy existovala slabina

Slabina nevznikne v operačním systému nebo aplikačním programu náhodou, sama od sebe. Jedná se počítačový program, takže zde neexistuje žádná únava materiálu a podobné důvody, které mohou být příčinou toho, že se skryté vady v hmotné výrobku projeví až po delší době.

Pokud pomineme záměrnou manipulaci v průběhu používání programu, tak slabina musí být v operačním systému nebo prohlížeči od uvedení na trh konkrétní verze programu.

Dobu existence slabiny jsme počítali od uvedení konkrétního programu na trh. V případě, že se slabina vyskytovala ve více verzích stejného programu, tak jsme brali jako počátek existence slabiny zveřejnění nejstarší verze příslušného programu, ve které byla slabina nalezena.

Při výpočtu dnů kdy existovala konkrétní slabina jsme úmyslně nepočítali přesně všechny dny existence slabiny. Takové výpočty jsou i zbytečné. Důležité je zda slabina existovala do 100 (150) dnů, do 300 dnů nebo déle jak rok nebo dokonce několik roků. Tyto dny jsou důležité při posuzování kdo (jaký typ útočníka) dokáže vytvořit nový škodlivý kód a zneužít příslušnou slabinu.

Důležitější je hrubý počet dnů a především zda se jedná o výjimku nebo o běžný způsob práce tvůrců počítačového programu.

Při posuzování doby objevení slabiny není možné brát vážně den kdy byla konkrétní slabina zveřejněna. Slabina (zadní vrátka) byla v programu již dříve a v konkrétní den se někdo rozhodl její popis zveřejnit. V minulosti jsme již zaznamenali případy, kdy byla slabina zneužívána a až v okamžiku kdy to počítačoví podvodníci přehnali a slabinu začali zneužívat k masovějším útokům, tak byla jejich činnost zaregistrována a následně byla zjištěna konkrétní slabina.

Proto navrhujeme počítat dobu existence slabiny již od okamžiku zveřejnění nejstarší verze, ve které se příslušná slabina objevila.

Analýza slabin
v operačních systémech a dalších programech, které byly zveřejněné v roce 2011

3 Použité zdroje informací.

Pro vypracování analýzy byly použity informace z veřejných zdrojů. Základním zdrojem informací byly www stránky tvůrců jednotlivých operačních systémů a prohlížečů www stránek. Dalším zdrojem byly stránky poradenských firem a stránky různých CERT (Computer Emergency Response Team).

3.1 Státní organizace a CERT

- National Vulnerability Database - http://nvd.nist.gov/
- Cyber Security Alerts - http://www.us-cert.gov/cas/alerts/
- Common Weakness Enumeration - http://cwe.mitre.org/index.html
- CERT Coordination Center (CERT/CC) - http://www.cert.org/cert/
- atd.

3.2 Výrobci operačních systémů a aplikačních programů

- Microsoft (Windows, MS Internet Explorer) - http://technet.microsoft.com/en-us/security/bulletin/
- Google (Chrome) - http://code.google.com/p/chromium/
- Mozila (Firefox) - http://www.mozilla.org/security/announce/2011/mfsa2011-50.html

4 Statistické podklady pro volbu zkoumaných programů

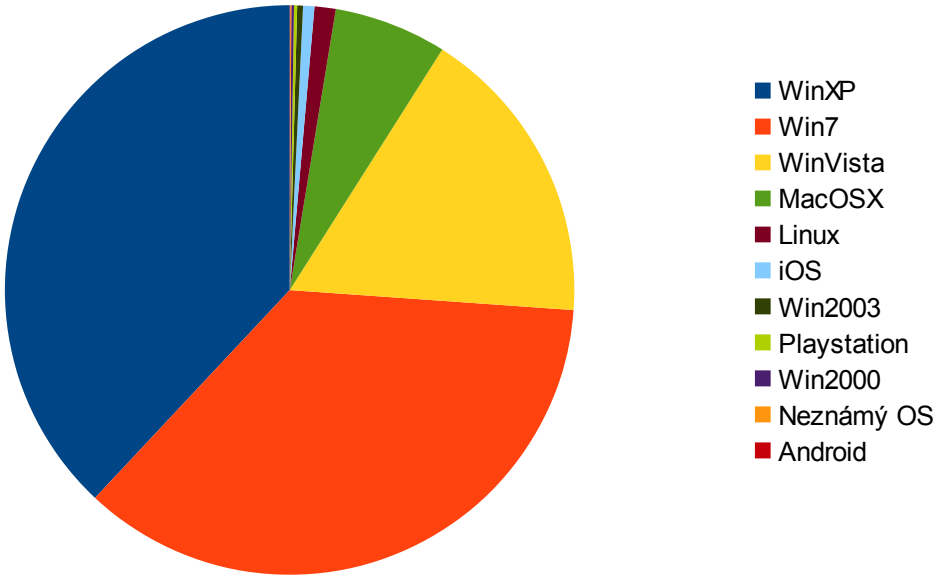
4.1 Zaměření analýzy

Kvalita softwaru nesmí být spojena s podílem na trhu. Vytvářet kvalitně naprogramovaný program bez zadních vrátek a slabin by měl být záměr každého programátora nebo týmu programátorů.

Na bezpečnost uživatelských počítačů má zásadní vliv kvalita operačního systému a prohlížeče www stránek. Z pohledu cíleného útoku na jednoho konkrétního uživatele (firmu) mohou být důležité i další, méně rozšířené programy a jejich kvalita. Z celkového pohledu jsou ale nejdůležitější operační systém a prohlížeč www stránek.

Z tohoto důvodu jsme analýzu zaměřili na operační systémy a browsery (prohlížeče www stránek)

4.2 Volba operačních systémů



Obrázek 1

Na obrázku č. 1 je vidět podíl jednotlivých operačních systémů na trhu.

Operační systém	Podíl na trhu
WinXP	38,01
Win7	35,82
WinVista	17,11
MacOSX	6,41
Linux	1,2
iOS	0,64
Win2003	0,33
Playstation	0,17
Win2000	0,15
Neznámý OS	0,07
Android	0,03

Tabulka 1

Jednotlivé průzkumy se mezi sebou mohou lišit hodnocením podílu mezi jednotlivými verzemi operačního systému Windows.

Všechny průzkumy se ale shodují v tom, že operační systém Windows verze XP, Vista a 7 jsou instalovány na více jak 90% uživatelských počítačů (desktop i notebook).

Do hodnocení slabin operačního systému jsme zahrnuly operační systémy **Windows** (7, Vista, XP).

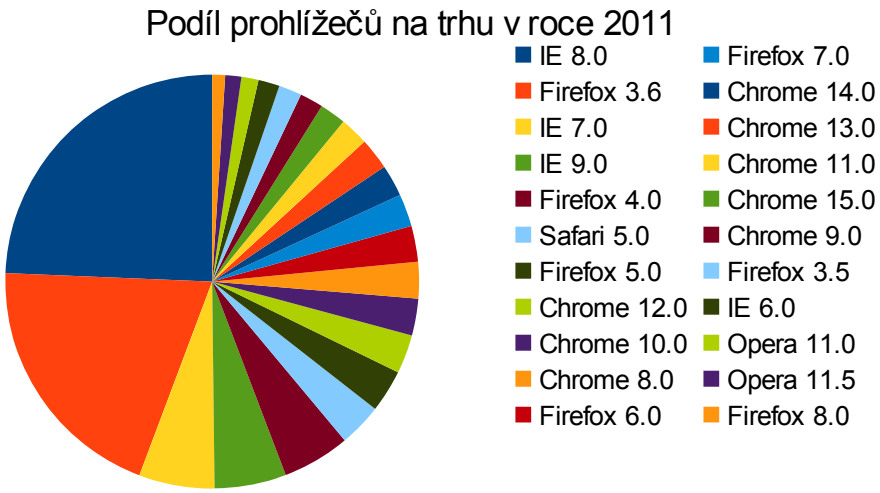
Jako zdroj informací o podílu jednotlivých operačních systémů na trhu osobních počítačů (desktop i notebook) jsme použili následující servery :

- Wikimedia Traffic Analysis Report - http://stats.wikimedia.org/wikimedia/squids/SquidReportOperatingSystems.htm
- NETMARKETSHARE - https://marketshare.hitslink.com/browser-market-share.aspx?qprid=2&qpcustomd=0
- StatCounter - http://gs.statcounter.com/

4.3 Volba prohlížečů

Vedle operačního systému je pro bezpečnost uživatelského počítače a pro bezpečnost jeho dat velmi důležitá kvalita browseru.

Vzhledem k rozsahu používání browseru pro obsluhu aplikací v lokální síti i v síti Internet představují chyby v prohlížečích velké nebezpečí.

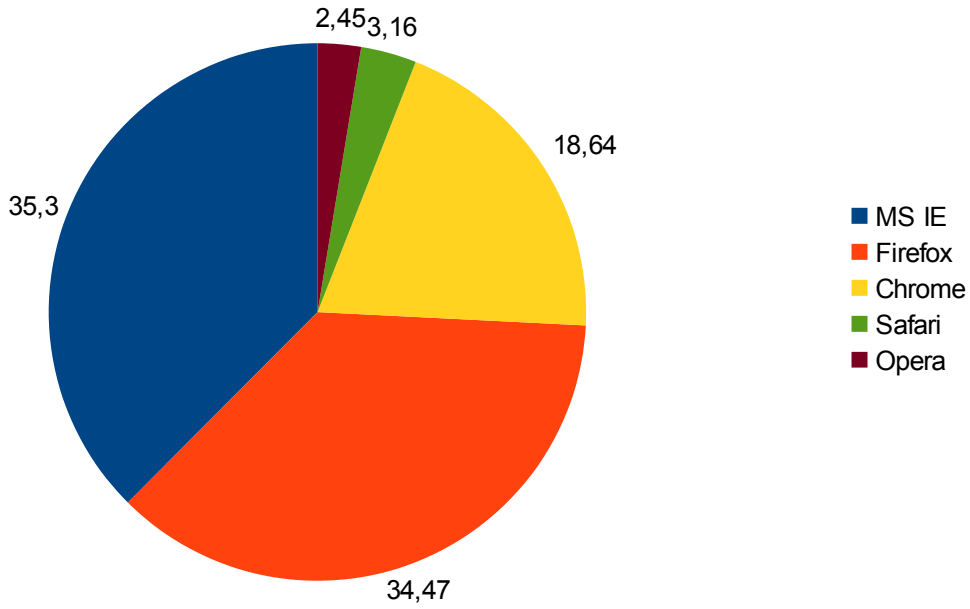


Obrázek 2

Na trhu browserů (prohlížečů www stránek) není situace tak jednoznačná jako v případě operačních systémů a podílu Windows.

IE 8.0	22,89%	Chrome 12.0	2,83%	Chrome 15.0	1,93%
Firefox 3.6	18,73%	Chrome 10.0	2,71%	Chrome 9.0	1,71%
IE 7.0	5,57%	Chrome 8.0	2,70%	Firefox 3.5	1,68%
IE 9.0	5,27%	Firefox 6.0	2,63%	IE 6.0	1,57%
Firefox 4.0	4,97%	Firefox 7.0	2,38%	Opera 11.0	1,26%
Safari 5.0	3,16%	Chrome 14.0	2,33%	Opera 11.5	1,19%
Firefox 5.0	3,14%	Chrome 13.0	2,33%	Firefox 8.0	0,94%
		Chrome 11.0	2,10%		

Tabulka 2



Obrázek 3

V oblasti browserů existuje větší konkurence než v případě operačních systémů. V případě prohlížečů www stránek jsou na trhu tři velké skupiny prohlížečů. Jedná se o Microsoft Internet Explorer, Mozila Firefox a relativně nový Google Crome, který velmi rychle zvyšuje svůj podíl na trhu.

Typ prohlížeče	Podíl na trhu
MS IE	35,3
Firefox	34,47
Chrome	18,64
Safari	3,16
Opera	2,45

Tabulka 3

Jako zdroj informací o podílu jednotlivých browserů na trhu jsme použili následující servery :

- Wikimedia Traffic Analysis Report - http://stats.wikimedia.org/wikimedia/squids/SquidReportOperatingSystems.htm
- NETMARKETSHARE - https://marketshare.hitslink.com/browser-market-share.aspx?qprid=2&qpcustomd=0
- StatCounter - http://gs.statcounter.com/

4.4 Vybrané operační systémy a prohlížeče www stránek

Vzhledem k podílu na trhu je zkoumání zaměřeno především na operační systémy společnosti Microsoft **Windows 7**, **Vista** a **XP** (případně 2000).

Vzhledem k podílu na trhu je zkoumání zaměřeno na prohlížeče www stránek Microsoft **Internet Explorer**, **Mozila Firefox** a **Google Chrome**.

* V analýze stavu za rok 2010 jsme v případě operačního systému Windows uváděli ještě srovnání s verzí Windows 2000. Vzhledem k tomu, že tvůrce operačního systému již neposkytuje technickou podporu verzi 2000 není možné z veřejných zdrojů ověřit zda se zveřejněná slabina vztahuje i k starému systému Windows 2000.

5 Operační systémy

V prostředí operačních systémů je situace již více jak 10 (deset) let téměř stejná. Společnost Microsoft se svým systémem Windows získala více jak 90% trhu stolních a přenosných počítačů. Ostatní se snaží, ale úspěch mají pouze u konkrétních skupin, jako například IT nadšenci, fanoušci „nakousnutého jablka“, atd.

Z pohledu obchodníka je 90% trhu obrovský úspěch. Na druhou stranu je to i závazek, když si uvědomíme, že počítač není pouze „chytrý“ psací stroj nebo přehrávač audio nebo video souborů. Počítače dnes běžně slouží pro obsluhu bankovního účtu, obchodování, komunikaci uvnitř firmy nebo s ostatními firmami a zhruba od nástupu Windows XP je vidět nasazování počítačů s různými operačními systémy a především s Windows do řízení technologických zařízení.

Dominantní postavení mimo jiné znamená, že slabina v takovém operačním systému nebo aplikaci znamená, že je ohroženo velké množství počítačů běžných uživatelů, počítačů v malých i větších firmách nebo dokonce řízení technologických celků, včetně například ovládání frekvenčních měničů centrifug.

Vzhledem k podílu na trhu je zkoumání zaměřeno na operační systémy společnosti Microsoft **Windows 7**, **Vista** a **XP** (případně 2000).

5.1 Analýza slabin v operačním systému Windows

V průběhu analýzy jsme zjistili, že v roce 2011 bylo zveřejněno a následně i opraveno 96 slabin, které se vztahovaly k operačnímu systému Windows 7.

	Počet slabin	
Pouze Win7	4 (96)	4,16%
Win7+Vista	9 (92)	9,38%
WIN7+ Vista+ XP	83	86,46%
Celkem	**96**	

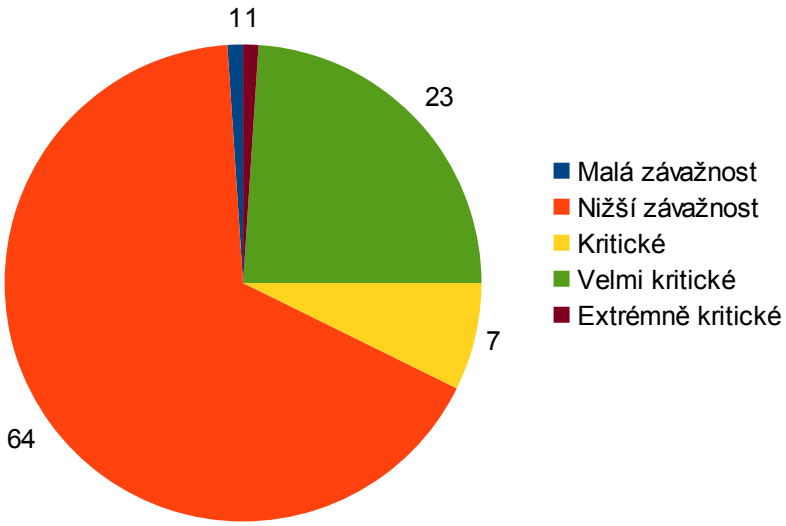
Tabulka 4

Ze zjištěných slabin se pouze 4 (čtyři) slabiny92 týkaly pouze verze Windows 7. Dalších 9 (devět) slabin bylo společných pro verze Windows 7 a Vista. Celkem 83 (osmdesát tři) slabin bylo společných pro tři po sobě jdoucí verze Windows tedy 7, Vista i XP. To tedy znamená, že 83 slabin bylo v operačním systému již od roku 2001, od uvedení verze Windows XP na trh. **83 slabin bylo v operačním systému 10 let než byly zveřejněny a opraveny.**

Obrázek 4

5.1.1 Charakter zranitelností zveřejněných v roce 2011 a jejich závažnost

Z 96 zveřejněných slabin bylo 31 slabin kritických, případně velmi kritických. Jedna slabina (CVE-2011-3402) byla hodnocena jako extrémně kritická. Extrémně kritická slabina byla společná pro Windows 7, Vista i XP. Z 30 dalších slabin bylo 23 velmi kritických, přičemž 18 slabin bylo opět společných pro verze 7, Vista i XP. Ze sedmi kritických slabin byly čtyři společné pro verze Windows 7, Vista i XP.



Obrázek 5

Z 96 slabin objevených a popsaných v roce 2011 bylo 31 slabin, které představovali vážné nebezpečí pro počítače běžných uživatelů, případně i pro počítače ve firemních sítích.

Celkem 23 slabin s hodnocením kritické, velmi kritické nebo extrémně kritické byly v operačních systémech minimálně od roku 2001, tedy od uvedení Windows XP na trh. Ze jištěných dat vyplývá, že v roce 2011 byly objeveny další 23 slabiny přes které bylo možné napadnout počítače běžných uživatelů, případně i firemní počítače nebo průmyslové aplikace ovládané prostřednictví aplikace pracující nad operačním systémem Windows.

Společné kritické chyby pro Win 7, Vista a XP

	Windows 7	7, Vista	7, Vista, XP
extrémně kritické	1	1	1
velmi kritické	23	22	18
kritické	7	5	4

Tabulka 5

5.1.2 Porovnání počtu slabin s rokem 2010

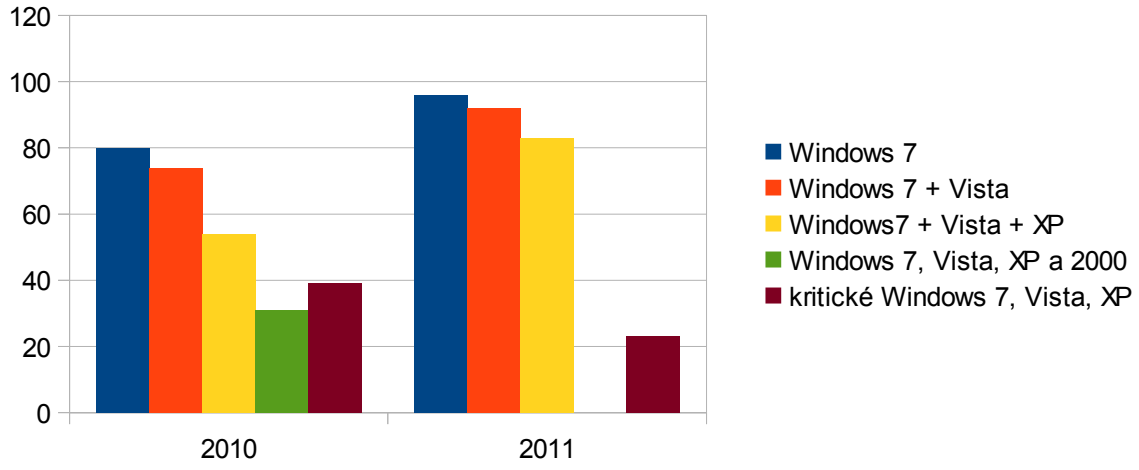
V seznamu zveřejněných slabin za rok 2010 jsme zjistili, že v operačním systému Windows 7 bylo objeveno a popsáno 80 chyb. Z těchto chyb bylo 74 slabin společných s verzí Vista a 54 slabin bylo společný i s verzí Windows XP. Dokonce 31 slabin bylo společných se starým operačním systémem Windows 2000.

Verze	Zjištěné chyby	Kritické chyby
Windows 7	80	53
Windows Vista	74	53
Windows XP	54	39
Windows 2000	31	23

Tabulka 6: Seznam slabin zveřejněných v roce 2010

Z 80 slabin zveřejněných v roce 2010 bylo 53 (padesát tři) slabin kritických, případně velmi kritických. Z nich bylo 39 (třicet devět) slabin společných pro verze Windows 7, Vista a XP. Dokonce 23 (dvacet tři) slabin bylo společných pro Windows 7 až Windows 2000.

Obrázek 6: Porovnání počtu slabin zveřejněných v roce 2010 a 2011



5.2 Shrnutí – operační systém

Útok na operační systém umožňuje získat kontrolu nad celým počítačem, resp. celým firemním informačním systémem nebo řídícím systémem.

Při analýze slabin zveřejněných v roce **2010** jsme zjistili 31 (54 s XP) slabin společných pro víc verzí a 23 (**39** s XP) případech se jednalo o kritické slabiny, které byly společné pro nejnovější Windows 7 a současně pro starý systém Windows 2000. Přičemž tento systém byl uveden na trh v roce 1999.

Při analýze slabin zveřejněných v roce **2011** jsme zjistili **83 slabin** společných pro verze Windows 7, Vista a XP a z toho a **23** slabin bylo kritických.

Při analýze v roce **2011** jsme již neměli podklady pro ověření zda se slabina týká pouze verzí Windows 7 – XP nebo i verze 2000. Společnost Microsoft přestala verzi 2000 podporovat a současně přestali zveřejňovat informace o slabinách v tomto systému.

Případný útočník měl v případě operačního systému Windows a slabin zveřejněných v roce 2011 více jak **3600 dnů** na odhalení těchto závažných slabiny, jejich otestování, vytvoření exploitu / škodlivého programu, který bude zneužívat tuto slabinu (slabiny), umístění škodlivého programu na počítač (počítače) oběti a skutečné zneužití slabiny.

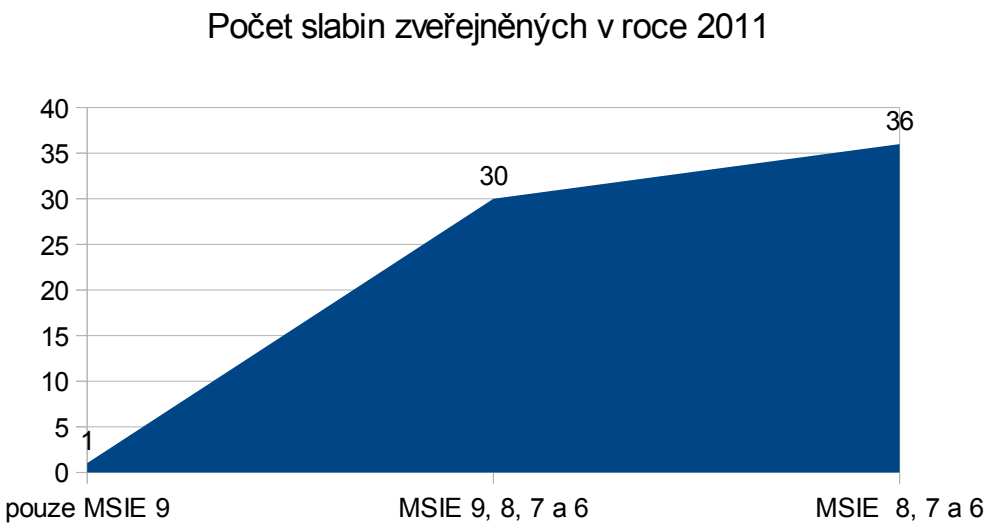
6 Prohlížeče

Od loňské analýzy došlo v oblasti prohlížečů, přesněji v oblasti uvádění nových verzí k rychlému vývoji.

- **Microsoft** vydal v březnu 2011 verzi 9 svého prohlížeče Internet Explorer
- **Mozilla** v průběhu roku 2011 vydala postupně šest nových verzí prohlížeče Firefox. Do loňské analýzy jsme zahrnuli verzi 3.6. V roce 2011 byly postupně vydány verze 4, 5, 6, 7, 8 a v prosinci ještě verze 9 Mozilla Firefox.
- **Google** uvedl na konci roku 2010 verzi 8.0 svého prohlížeče Chrome. V průběhu roku 2011 byly postupně vydávány nové verze 9 – 16 (šestnáct).

6.1 Microsoft Internet Explorer

Obrázek 7



	Počet slabin		
	pouze MSIE 9	MSIE 9, 8, 7 a 6	MSIE 8, 7 a 6
	1	30	30+6
Celkem	**1**	**30**	**36**

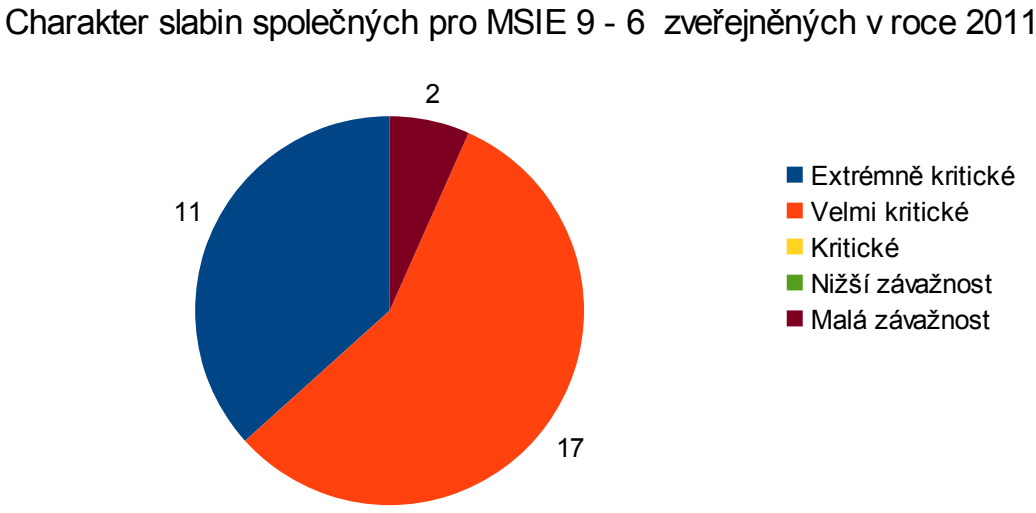
Tabulka 7

V analýze za roku 2010 jsme posuzovali verzi 8.0 Proto i v letošní analýze jsme s věnovali verzi 8.0 a současně i nové verzi 9.0. Zjistili jsme, že pouze jedna slabina se týkala pouze verze 9.0.

Žádná slabina se netýkala pouze verze 8.0, přesněji všechny slabiny zjištěné v roce 2011 ve verzi Microsoft Internet Explorer 8.0 se týkaly i starších verzí MSIE 7 a MSIE 6. Jednalo se o 36 (třicet šest) slabin společných pro MSIE 8, 7 a 6.

V prohlížeči MSIE 9 bylo zveřejněna 31 (třicet jedna) slabina, přičemž 30 (třicet) ze zveřejněných slabin bylo společných i pro verze 8, 7 a 6. Microsoft Internet Explorer 6 byl uveden na trh v srpnu 2001. Takže slabiny byly v prohlížeči 10 (deset) let.

Vzhledem k ukončení technické podpory prohlížeče MSIE 5.0 (5.01, 5.5) ze strany společnosti Microsoft jsme nemohli posoudit zda jsou zjištěné slabiny v novějších verzích společné i pro prohlížeč z roku 1999.



Obrázek 8

Charakter slabin společných pro MSIE 9 - 6

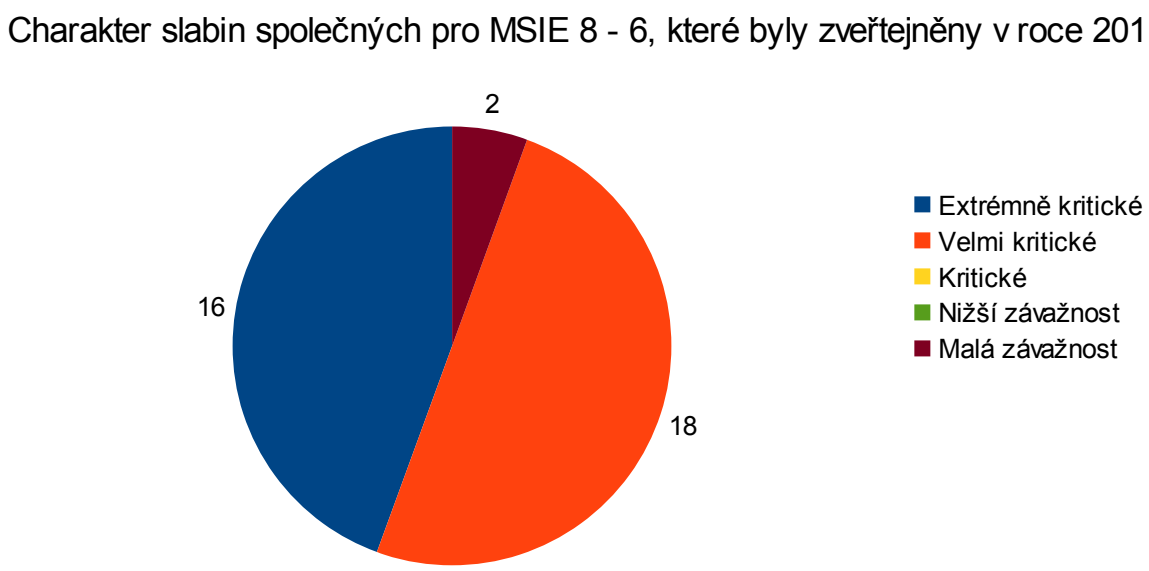
Extrémně kritické	Velmi kritické	Kritické	Nižší závažnost	Malá závažnost
11	17	0	0	2

Tabulka 8

Z **30** (třiceti) slabin společných pro verze 9 – 6 Internet Exploreru měly pouze dvě slabiny malou závažnost. Ostatních **28** (dvacet osm) slabin bylo velmi kritických nebo dokonce extrémně kritických. Zneužití těchto slabin mohlo znamenat vážné nebezpečí pro počítač běžného uživatele i pro počítač nebo lokální síť spravovanou průměrně zkušeným administrátorem.

Charakter slabin společných pro MSIE 8 - 6				
Extrémně kritické	Velmi kritické	Kritické	Nižší závažnost	Malá závažnost
16	18	0	0	2

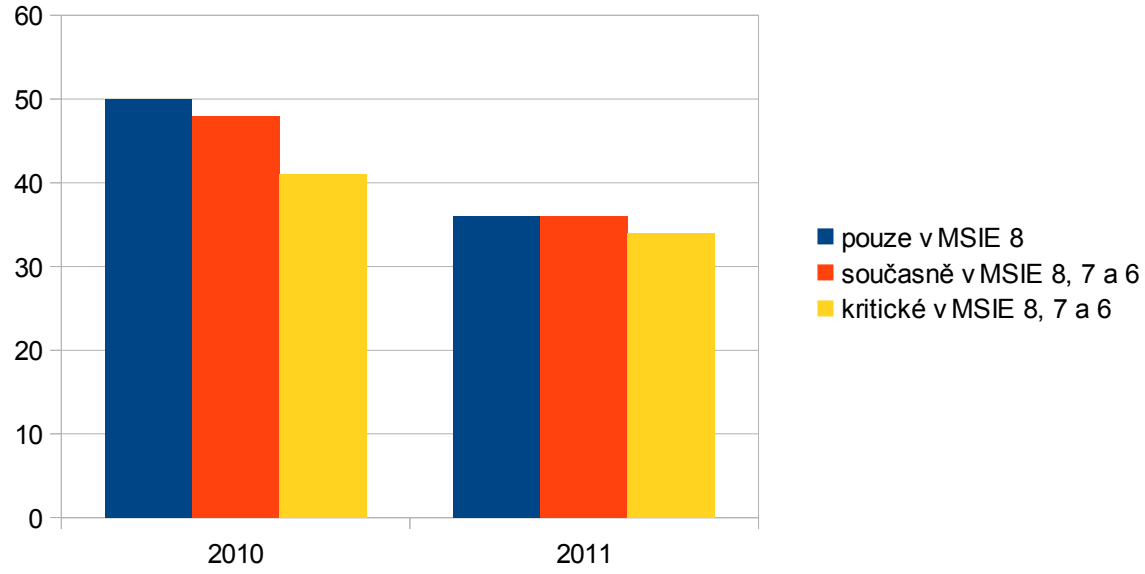
Tabulka 9



Obrázek 9

Z **36** (třiceti šesti) slabin společných pro verze 8 – 6 Internet Exploreru měly pouze dvě slabiny malou závažnost. Ostatní **34** (třicet čtyři) slabiny byly velmi kritické nebo dokonce extrémně kritické.

Při zkoumání slabin zveřejněných v roce 2010 v prohlížeči MSIE 8.0 jsme zjistili celkem 50 slabin. Z těchto slabin bylo **48** (čtyřicet osm) slabin společných pro poslední tři verze (8,7,6), přičemž **41** (čtyřicet jedna) slabina měly charakter velmi kritických nebo extrémně kritických slabin.

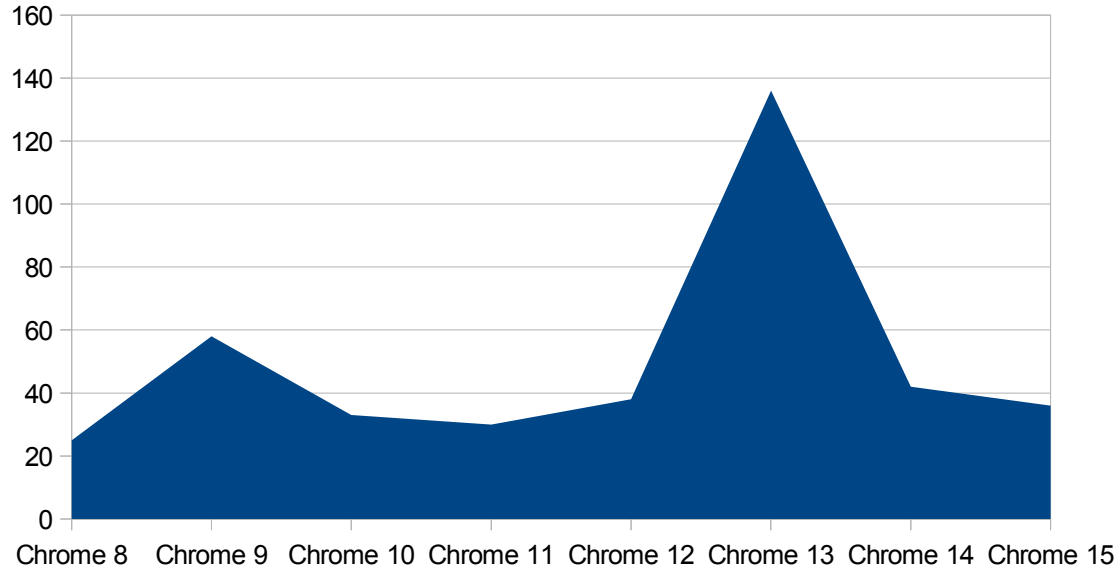


Obrázek 10

V letech 2010 a 2011 bylo v prohlížečích MSIE zveřejněno celkem 75 (sedmdesát pět) velmi kritických nebo extrémně kritických slabin, které byly společné pro verzi MSIE 8 a verzi MSIE 6. To tedy znamená, že 75 velmi vážných slabin bylo v tomto prohlížeči minimálně 10 (deset) let.

Případný útočník měl v případě MSIE 6-9 a slabin zveřejněných v roce 2011 více jak **3600 dnů** na odhalení závažné slabiny, její otestování, vytvoření exploitu / škodlivého programu, který bude zneužívat tuto slabinu (slabiny), umístění škodlivého programu na počítač (počítače) oběti a skutečné zneužití slabiny.

6.2 **Google Chrome**

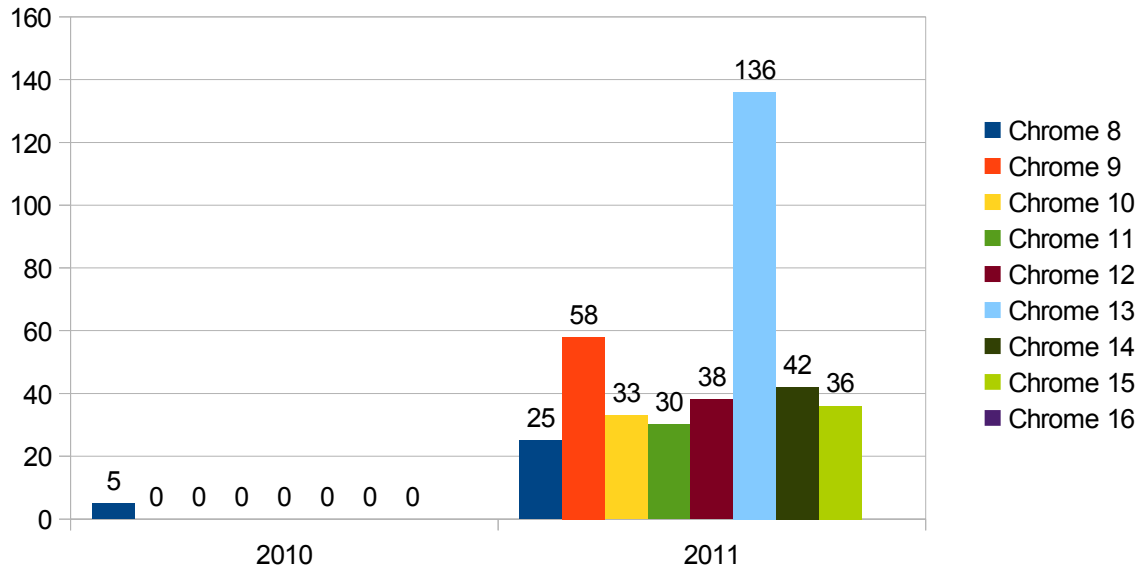


Tabulka 10: Chyby v prohlížeči Google Chrome ve verzích uvolněných v roce 2011

V případě prohlížeče Google Chrome byla v roce 2010 jako poslední uvedena verze 8. Již tato verze neměla v roce 2010 žádnou z 5 (pěti) zveřejněných slabin společnou s předchozími verzemi.

V roce 2011 bylo postupně zveřejněno 9 (devět) nových verzí prohlížeče Google Chrome, tedy verze číslo 9 -16.

V průběhu analýzy jsme zjistili téměř 400, přesně 398 slabin, které se týkají různých verzí prohlížečů Google Chrome od verze 9 až po 16. Nezjistili jsme žádnou slabinu, která by se vyskytovala v několika po sobě jdoucích verzích. Každá ze zjištěných 398 slabin se vztahovala pouze k jedné verzi prohlížeče Google Chrome.



Obrázek 11: Počty slabin v roce 2010 a 2011

Charakter slabin společných Chrome 15-12

Extrémně kritické	Velmi kritické	Kritické	Nižší závažnost	Malá závažnost
0	0	0	0	0

Tabulka 11 : V prohlížeči Google Chrome nebyla zveřejněna společná chyba pro několik posledních verzí

V roce 2011 bylo v prohlížeči Google Chrome zveřejněno celkem téměř 400 slabin. ale doba pro zneužití konkrétní slabiny byla vždy relativně krátká.

Doba mezi vydáním jednotlivých verzí nepřesáhla 2 měsíce, přesně 63 dnů. Současně nové verze prohlížeče nemají společné slabiny s předchozími verzemi.

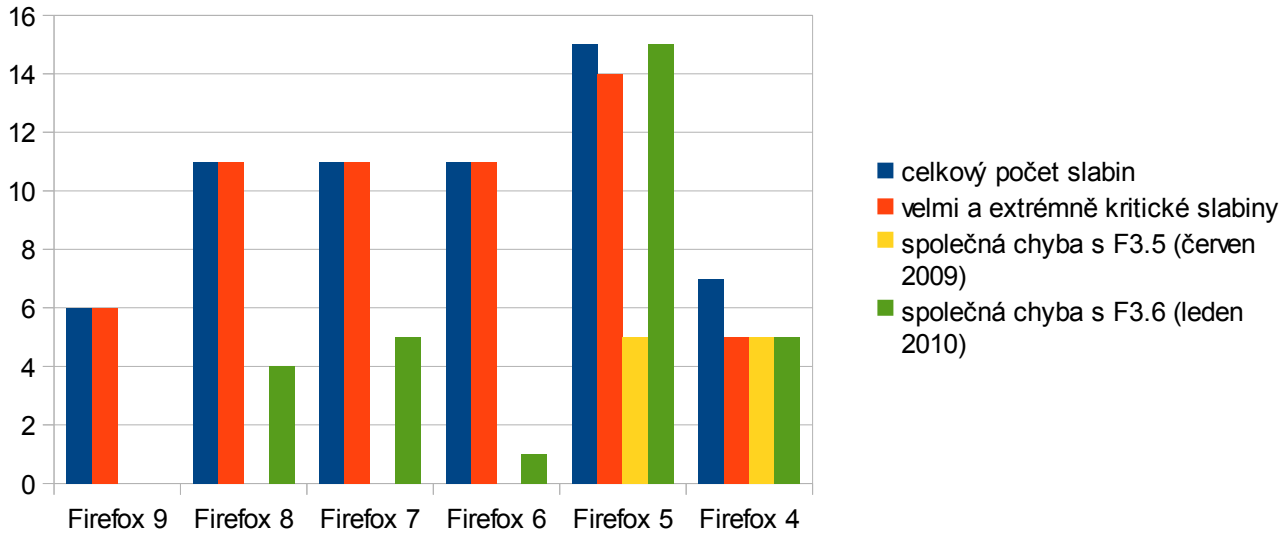
- Google Chrome – 8.0 vydán 2. prosince 2010
  - **63 dnů**
- Google Chrome – 9.0 vydán 3. února 2011
  - **33 dnů**
- Google Chrome – 10.0 vydán 8. březen 2011
  - **50 dnů**
- Google Chrome – 11.0 vydán 27. dubna 2011
  - **41 dnů**
- Google Chrome – 12.0 vydán 7. června 2011
  - **56 dnů**
- Google Chrome – 13.0 vydán 2. srpna 2011
  - **46 dnů**
- Google Chrome – 14.0 vydán 16. září 2011
  - **40 dnů**
- Google Chrome – 15.0 vydána 25. října 2011
  - **49 dnů**
- Google Chrome – 16.0 vydán 13. prosince2011

Tabulka 12: Počet dnů mezi vydáním jednotlivých verzí Google Chrome

To tedy znamená případná slabina byla v prohlížeči Google Chrome v roce 2011 maximálně dva měsíce. Potenciální útočník by měl v roce 2011 maximálně **63 dnů na odhalení závažné slabiny**, vytvoření exploitu / škodlivého programu, jeho otestování, umístění na počítač (počítače) oběti a skutečné zneužití konkrétní slabiny dříve než by byl prohlížeč aktualizován na novou verzi. To je velmi krátká doba.

6.3 Mozilla Firefox

Obrázek 12: Slabiny v prohlížeči Firefox v roce 2011



V případě prohlížeče Mozilla Firefo byla v roce 2010 jako poslední uvedena verze 3.6. V roce 2011 bylo postupně zveřejněno 5 (pět) nových verzí prohlížeče Mozilla Firefox, tedy verze číslo 4, 5, 6, 7 a 8.

V průběhu analýzy jsme zjistili téměř 100, přesně 96 slabin, které byly zveřejněny v roce 2011 a týkají se prohlížečů Mozilla Firefox od verze 4 až po verzi 9.

Ve verzích Firefox 4 a 5 byly objeveny společné slabiny s verzí Firefox 3.5, která byla vydána v červnu 2010. Ve verzích 8 - 4 prohlížeče Firefox, které byly vydány v roce 2011 byly nalezeny a otestovány slabiny společné s verzí Firefox 3.6, která byla vydána v lednu 2010.

Slabina společná s verzí Firefox 3.0 nebo staršími nebyla nalezena.

Potenciální útočník by měl v případě slabin společných pro Firefox 3.6 a 8.0 zhruba **700 dnů na odhalení závažné slabiny**, vytvoření exploitu / škodlivého programu, jeho otestování, umístění na počítač (počítače) oběti a skutečné zneužití konkrétní slabiny dříve než by byl prohlížeč aktualizován na novou verzi.

V případě verze 9 bylo zveřejněno **6** (šest) slabin. Všech **6** (šest) slabin bylo kritických. Žádná ze zveřejněných slabin nebyla společná s žádnou z předchozích verzích prohlížeče Firefox. Tato slabina byla v prohlížeči necelý měsíc, tedy méně než **30** dnů.

	Firefox 9	Firefox 8	Firefox 7	Firefox 6	Firefox 5	Firefox 4
celkový počet slabin	6	11	11	11	15	7
velmi a extrémně kritické slabiny	6	11	11	11	14	5
společná chyba s F3.5 (červen 2009)	0	0	0	0	5	5
společná chyba s F3.6 (leden 2010)	0	4	5	1	15	5

Tabulka 13: Slabiny v prohlížeči Mozilla Firefox, které byly zveřejněny v roce 2011

6.4 Shrnutí - prohlížeče

Microsoft Internet Explorer 9.0

V případě prohlížeče Microsoft (Windows) Internet Explorer 9 jsme v průběhu analýzy zjistili celkem **31** (třicet jedna) slabin v poslední verzi prohlížeče, z čehož bylo **28** (dvacet osm) slabin bylo kritických. Velmi alarmující je zjištění, že **28** (dvacet osm) slabin, které byly zveřejněné v roce 2011 a **48** slabin objevených v roce 2010 bylo v prohlížeči MSIE více jak **3500 dnů** aniž by tyto slabiny někdo zveřejnil a opravil.

Google Chrome 16

V případě prohlížeče Google Chrome a jeho aktuální verze číslo 16 jsme v průběhu analýzy nezjistil slabinu. V průběhu roku 2011 bylo zveřejněno celkem **398** slabin v různých verzích prohlížeče Google Chrome. Žádná zjištěná slabina nebyla společná pro dvě verze prohlížeče Google Chrome.

V případě Google Chrome jsme nezjistili slabinu společnou se staršími verzemi prohlížeče Chrome. Maximální doba existence slabiny byla **63 dnů.**

Mozila Firefox 9.0 a 8.0

V případě verze 9.0 bylo zveřejněno **6** (šest) slabin. Všech **6** (šest) slabin bylo kritických. Žádná ze zveřejněných slabin nebyla společná s žádnou z předchozích verzích prohlížeče Firefox. Tato slabina byla v prohlížeči necelý měsíc, tedy méně než **30** dnů.

V případě předchozí verze prohlížeče Mozilla Firefox (verze 8.0)jsme v průběhu analýzy zjistil celkem **11** slabin, přičemž všech **11** slabin bylo kritických. Všech 11 slabin bylo společných s verzí Firefox 3.6. To znamená, že případný útočník měl dva roky, zhruba **700 dnů** na odhalení a zneužití slabiny společné pro verzi 8 a 3.6.

7 Závěr

V průběhu analýzy jsme zjistili, že přístup k využívání zdrojových kódů se u jednotlivých tvůrců zkoumaných programů velmi liší. Na jedné straně jsou prohlížeče, ve kterých byly slabiny maximálně dva měsíce, na druhé straně je prohlížeč a operační systém, ve kterém byly slabiny deset a více let než byly zveřejněny a opraveny. Zjištěné skutečnosti jsou velmi alarmující.

Slabiny, které byly v operačním systému Windows více jak deset let jsou i vysvětlením toho jak se mohl do té doby neznámý škodlivý program dostat do relativně dobře zabezpečeného počítače běžných uživatelů, do lokálních sítí firem nebo dokonce do systémů, které řídí aplikace v průmyslu.

Útok přes zneužití zatím neznámé slabiny je mimo jiné nebezpečný v tom, že takový průnik do operačního systému není vidět a nemusí jej detekovat ani bezpečnostní programy. Tlak na tvůrce počítačových programů a tlak na zkrácení doby existence slabin v operačních systémech a aplikačních programech pomůže ke snížení počtu těch nejzávažnějších počítačových útoků.

Autor analýzy :

Jiří Nápravník

SALAMANDR
Josefodolská 490
582 91 Světlá nad Sázavou
tel : +420 569456498, +420 603851266
e-mail : napravnik.jiri@salamandr.cz
www.salamandr.cz

8 O autorovi analýzy

Jiří Nápravník (*1968)

Oblasti počítačů a bezpečnosti informačních systémů s dopady na fungování firem se věnuje od počátku 90. let.

Počátkem 90. let pracoval ve Vojenském výzkumném ústavu a později na Burze cenných papírů Praha, a.s. Posléze pracoval na pozicích bezpečnostního specialisty, následně tvůrce a vedoucího oddělení bezpečnosti informačních systémů u významného českého systémového integrátora. V roce 1997 byl jmenován soudním znalcem v oborech výpočetní technika a počítačová kriminalita. V uplynulých letech se jako soudní znalec podílel na objasňování více jak patnácti případů podvodů s použitím počítačů a Internetu. V letech 2002-06 se podílel na úspěšném vyšetření případů, kdy došlo k vykradení bankovních účtů prostřednictvím internetového bankovnictví. V letech 2006 -2008 pracoval jako ředitel výrobních závodů v Jihlavě a ve Světlé nad Sázavou pro švédskou společnost Svenska Cellulosa Aktiebolaget (SCA Packaging). V roce 2010 jako interim manager v Lev Foundry Halić.

Od roku 2009 pracuje jako konzultant v oblasti zjednodušování vnitrofiremních pracovních postupů a v oblasti využívání informačních systémů.

Přílohy
seznam slabin CVE-2011- …

Příloha č. 1 : Seznam slabin ve Windows 7, které byly zveřejněny v roce 2011

CVE-2011-2016	CVE-2011-1874	CVE-2011-0666	CVE-2011-1239
CVE-2011-2004	CVE-2011-1875	CVE-2011-0667	CVE-2011-1240
CVE-2011-2004	CVE-2011-1876	CVE-2011-0670	CVE-2011-1241
CVE-2011-2013	CVE-2011-1877	CVE-2011-0671	CVE-2011-1242
CVE-2011-3402	CVE-2011-1878	CVE-2011-0672	CVE-2011-0034
CVE-2011-1985	CVE-2011-1879	CVE-2011-0673	CVE-2011-0661
CVE-2011-2002	CVE-2011-1880	CVE-2011-0674	CVE-2011-0657
CVE-2011-2003	CVE-2011-1881	CVE-2011-0675	CVE-2011-0663
CVE-2011-2011	CVE-2011-1882	CVE-2011-0676	CVE-2011-0032
CVE-2011-2009	CVE-2011-1883	CVE-2011-0677	CVE-2011-0042
CVE-2011-1247	CVE-2011-1884	CVE-2011-1225	CVE-2011-0029
CVE-2011-3389	CVE-2011-1885	CVE-2011-1226	CVE-2011-0654
CVE-2011-1991	CVE-2011-1886	CVE-2011-1227	CVE-2011-0660
CVE-2011-1971	CVE-2011-1887	CVE-2011-1228	CVE-2011-0033
CVE-2011-1871	CVE-2011-1888	CVE-2011-1229	CVE-2011-0031
CVE-2011-1965	CVE-2011-1894	CVE-2011-1230	CVE-2011-0091
CVE-2011-1967	CVE-2011-1267	CVE-2011-1231	CVE-2011-0086
CVE-2011-1975	CVE-2011-1869	CVE-2011-1232	CVE-2011-0087
CVE-2011-1281	CVE-2011-1268	CVE-2011-1233	CVE-2011-0088
CVE-2011-1282	CVE-2011-0658	CVE-2011-1234	CVE-2011-0089
CVE-2011-1283	CVE-2011-1873	CVE-2011-1235	CVE-2011-0090
CVE-2011-1284	CVE-2011-1249	CVE-2011-1236	CVE-2011-0096
CVE-2011-1270	CVE-2011-0662	CVE-2011-1237	CVE-2011-0027
CVE-2011-1265	CVE-2011-0665	CVE-2011-1238	CVE-2011-0026

víc na adrese - http://cve.mitre.org

Příloha č. 2 : Seznam slabin v Microsoft Internet Exploreru verze 9 (8) zveřejněných v roce 2011

CVE-2011-1992	CVE-2011-1257	CVE-2011-1255
CVE-2011-2019	CVE-2011-1347	CVE-2011-1256
CVE-2011-3404	CVE-2011-1960	CVE-2011-1258
CVE-2011-5071	CVE-2011-1961	CVE-2011-1260
CVE-2011-4689	CVE-2011-1962	CVE-2011-1261
CVE-2011-1993	CVE-2011-1963	CVE-2011-1262
CVE-2011-1995	CVE-2011-1964	CVE-2011-1266
CVE-2011-1996	CVE-2011-1246	CVE-2011- 0094
CVE-2011-1997	CVE-2011-1250	CVE-2011- 0346
CVE-2011-1999	CVE-2011-1251	CVE-2011- 1244
CVE-2011-2000	CVE-2011-1252	CVE-2011- 1245
CVE-2011-2001	CVE-2011-1254	CVE-2011- 1345
CVE-2011-2383		

víc na adrese - http://cve.mitre.org

Seznam slabin zveřejněných v roce 2011 v prohlížeči Mozilla Firefox

CVE-2011-3647	CVE-2011-2368	CVE-2011-1202	CVE-2011-3866
CVE-2011-3648	CVE-2011-2369	CVE-2010-1585	CVE-2011-3232
CVE-2011-3650	CVE-2011-2370	CVE-2011-0051	CVE-2011-3005
CVE-2011-2372	CVE-2011-2371	CVE-2011-0053	CVE-2011-3004
CVE-2011-2995	CVE-2011-2373	CVE-2011-0054	CVE-2011- 3003
CVE-2011-2996	CVE-2011-2374	CVE-2011-0051	CVE-2011-3002
CVE-2011-2998	CVE-2011-2375	CVE-2011-0056	CVE-2011-2997
CVE-2011-2999	CVE-2011-2376	CVE-2011-0057	CVE-2011- 2372
CVE-2011-3000	CVE-2011-2377	CVE-2011-0058	
CVE-2011-3001	CVE-2011-2605	CVE-2011-0059	CVE-2011-2993
CVE-2011-3867	CVE-2011-0065	CVE-2011-0061	CVE-2011-2992
CVE-2011-0084	CVE-2011-0066	CVE-2011-0062	CVE-2011- 2991
CVE-2011-2378	CVE-2011-0067	CVE-2011- 2598	CVE-2011-2990
CVE-2011-2980	CVE-2011-0069	CVE-2011-4688	CVE-2011- 2989
CVE-2011-2981	CVE-2011-0070	CVE-2011-3658	CVE-2011- 2988
CVE-2011-2982	CVE-2011-0071	CVE-2011-3660	CVE-2011- 2987
CVE-2011-2983	CVE-2011-0072	CVE-2011-3661	CVE-2011- 2986
CVE-2011-2984	CVE-2011-0073	CVE-2011-3663	CVE-2011- 2985
CVE-2011-0083	CVE-2011-0074	CVE-2011-3664	CVE-2011- 0084
CVE-2011-0085	CVE-2011-0075	CVE-2011-3665	
CVE-2011-2362	CVE-2011-0076	CVE-2011- 3649	
CVE-2011-2363	CVE-2011-0077	CVE-2011- 3651	
CVE-2011-2364	CVE-2011-0078	CVE-2011- 3652	
CVE-2011-2365	CVE-2011-0079	CVE-2011- 3653	
CVE-2011-2366	CVE-2011-0080	CVE-2011- 3654	
CVE-2011-2367	CVE-2011-0081	CVE-2011- 3655	

víc na adrese - http://cve.mitre.org