Mesačný prehľad kritických zraniteľností
Január 2015

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2015-0014 služby Telnet spôsobená nesprávnou kontrolou používateľského vstupu. Útočník môže odoslaním škodlivého packetu spôsobiť pretečenie vyrovnávacej pamäte (buffer overflow), ktoré umožňuje vzdialené spustenie škodlivého kódu.
Služba Telnet je štandardne nainštalovaná na operačných systémoch Windows Server 2003, na systémoch Windows Vista a na novších štandardne nainštalovaná nie je.

Zraniteľné systémy:

Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8 for 32-bit Systems
Windows 8 for x64-based Systems
Windows 8.1 for 32-bit Systems
Windows 8.1 for x64-based Systems
Windows RT
Windows RT 8.1
Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 with SP2 for Itanium-based Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-based Systems Service Pack 2
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)

Odporúčania:

Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedenú zraniteľnosť sú distribuované pod označením MS15-002. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si januárový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/library/security/MS15-002

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft nevydala v mesiaci január žiadne bezpečnostné aktualizácie produktov Microsoft Office a Office Web Apps.

Spoločnosť Microsoft publikovala upozornenie na zvýšený výskyt emailov so škodlivou prílohou, obsahujúcou malvér, ktorý zneužíva funkcionalitu makier v produktoch Microsoft Office. Po otvorení škodlivého dokumentu v MS Office s povolenými makrami je možné spustenie, alebo stiahnutie a spustenie škodlivého kódu.

Odporúčania:
Nepovoľovať makrá pre nedôveryhodné súbory a nespúšťať nepodpísané makrá.
Makrá sú štandardne v MS Office z bezpečnostných dôvodov zakázané. Overenie nastavenia a prípadné zakázanie makier je možné v menu aplikácie MS Office:
Možnosti aplikácie Word/Excel -> Centrum zabezpečenia -> Nastavenia Centra zabezpečenia -> Nastavenie makier -> Zakázať všetky makrá s oznámením
Dokumenty obsahujúce faktúry, potvrdenia a iné finančné informácie zväčša nepotrebujú funkcionalitu makier. Je potrebné byť obozretný pri otváraní e-mailových príloh s touto tematikou, najmä ak ide o neovereného odosielateľa.

Zdroje:
https://technet.microsoft.com/library/security/ms15-jan
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=125

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na zraniteľnosti prehrávača Adobe Flash Player v programe Internet Explorer na základe aktualizácie, ktoré vydala spoločnosť Adobe (bližšie informácie v časti 4. Adobe Flash Player)

Zraniteľné systémy:
Microsoft Internet Explorer 10-11 (Adobe Flash Player)

Odporúčania:
Spoločnosť Microsoft zverejnila aktualizácie prostredníctvom bežného kanála Windows Update. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si Microsoft Security Advisory dostupné na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/library/security/2755801.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala novú verziu prehliadača Firefox opravujúcu 9 zraniteľností, z toho sú tri označené ako kritické.
Zraniteľnosť CVE-2014-8643 umožňuje v operačných systémoch Windows obísť sandbox Gecko Media Plugin, ktorý sa používa na prehrávanie videí vo formáte h.264.
Zraniteľnosť CVE-2014-8641 je spôsobená opätovným čítaním už uvoľnenej pamäte v komponente WebRTC a môže byť zneužitá na vzdialené spustenie škodlivého kódu.
Viaceré bližšie nešpecifikované zraniteľnosti pri práci s pamäťou umožňujúce útočníkovi spôsobiť pád aplikácie a možné spustenie škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 34 a predchádzajúce
Mozilla Firefox ESR 31.3 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 35.0.1 a Mozilla Firefox ESR 31.4)
Aktualizácia prehliadača by sa mala nainštalovať automaticky, pokiaľ sa tak nestalo, aktualizujte manuálne kliknutím na Firefox menu, ponuku Pomocníka a O prehliadači Firefox. Zobrazí sa okno s informáciou o používanej verzii prehliadača, súčasne sa skontrolujú a následne stiahnu aktualizácie.

Zdroje:
https://www.mozilla.org/sk/security/advisories/

Google Chrome

Spoločnosť Google vydala štyri aktualizácie prehliadača Chrome, ktoré obsahujú opravy zraniteľností prehrávača Adobe Flash Player a tiež dalších 62 bezpečnostných opráv. Najzávažnejšie zraniteľnosti sú spôsobené poškodením pamäte, resp. opätovným použitím uvoľnenej pamäte pri spracovávaní regulárnych výrazov, pri práci s IndexedDB, WebAudio a v JavaScriptovom jadre V8. Nájdené zraniteľnosti umožňujú vzdialeným útočníkom vykonať útoky typu zamietnutie služby (spôsobiť pád aplikácie), prípadne môžu mať iný bližšie nešpecifikovaný dôsledok.

Zraniteľné systémy
Google Chrome do verzie 40.0.2214.91

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 40.0.2214.93, prípadne po dôkladnom otestovaní na najnovšiu verziu 40.0.2214.94. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2015/01/stable-channel-update.html
http://googlechromereleases.blogspot.in/2015/01/stable-update.html
http://googlechromereleases.blogspot.in/2015/01/stable-channel-update_26.html
http://googlechromereleases.blogspot.in/2015/01/stable-channel-update_30.html

4. Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci január tri aktualizácie opravujúce 10 zraniteľností. Väčšina zraniteľnosti je spôsobená rôznymi chybami pri práci s pamäťou. Zraniteľnosti umožňujú vzdialenému útočníkovi spustenie škodlivého kódu a odhalenie citlivých informácií (stlačené klávesy na klávesnici).
Opravené sú aj zraniteľnosti CVE-2015-0310 a CVE-2015-0311, ktoré sú spôsobené chybami pri práci s pamäťou (neuvoľňovanie pamäte, použitie uvoľnenej pamäte). Na uvedené zraniteľnosti boli zaznamenané exploity, pomocou ktorých mohol vzdialený útočník obísť ochranu ASLR na platforme Windows a spustiť škodlivý kód.

Zraniteľné systémy
Adobe Flash Player do verzie 16.0.0.287
Adobe Flash Player do verzie 13.0.0.262
Adobe Flash Player do verzie 11.2.202.438

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 16.0.0.296, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 13.0.0.264. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.440.
Aktualizáciu odporúčame vykonať čo najskôr, nakoľko bolo zaznamenané použitie exploitov na niektoré zraniteľnosti.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player 16.x.

Zdroje:
http://helpx.adobe.com/security/products/flash-player/apsb15-01.html
http://helpx.adobe.com/security/products/flash-player/apsb15-02.html
http://helpx.adobe.com/security/products/flash-player/apsb15-03.html

Aktualizácia 2. februára 2015:
Bol objavený exploit na 0day zraniteľnosť v aktuálnej verzii Adobe Flash Player 16.0.0.296. V čas písania tejto správy nie je dostupná žiadna záplata na nájdenú zraniteľnosť CVE-2015-0313 ani odporúčania na zmiernenie rizika, preto odporúčame dočasne zakázať prehrávač Adobe Flash Player.

http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=128

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft nevydala v mesiaci január žiadne bezpečnostné aktualizácie platformy .NET.

Zdroje:
https://technet.microsoft.com/library/security/ms15-jan

Oracle Java

Spoločnosť Oracle vydala pravidelnú štvrťročnú sadu aktualizácií na zraniteľnosti Java SE. Najzávažnejšie zraniteľnosti komponentov Hotspot, JAX-WS, Libraries a RMI s označeniami CVE-2014-6601, CVE-2015-0412, CVE-2014-6549, CVE-2015-0408, CVE-2015-0395 a CVE-2015-0437 umožňujú vzdialené spustenie škodlivého kódu a prevzatie kontroly nad operačným systémom obete.

Zraniteľné systémy:
Java SE 5.0u75
Java SE 6u85
Java SE 7u72
Java SE 8u25

Odporúčania:
Spoločnosť Oracle zverejnila aktualizáciu prostredníctvom bežného kanála Java Auto Update. Aktualizácie sú dostupné aj na stránke java.com. Používateľom odporúčame nainštalovať najnovšie verzie Java SE 8 Update 31, resp. Java SE 7 Update 75. Upozorňujeme však, že po apríli 2015 už nebudú dostupné verejné aktualizácie platformy Java SE 7.

Zdroje:
http://www.oracle.com/technetwork/topics/security/alerts-086861.html
http://java.com/en/download/manual_java7.jsp

6. Iné závažné zraniteľnosti

Zvýšený výskyt ransomware

V mesiaci január zaznamenali CSIRT.SK a antivírusové spoločnosti zvýšený výskyt ransomware a tiež kampaň využívajúcu nový variant škodlivého kódu CTB-Locker, ktorý sa šíri prostredníctvom spamových emailov aj na Slovensku.
Vo všeobecnosti ransomware po úspešnom infikovaní zariadenia šifruje jeho obsah (pričom sa môže zamerať iba na súbory určitého typu). Po zašifrovaní zobrazí upozornenie používateľovi, od ktorého žiada výkupné za sprístupnenie zašifrovaných súborov.

Odporúčania:
Pre zníženie rizika odporúčame nasledovné opatrenia:

- neuvádzajte neuvážene svoj e-mailový kontakt na rôznych webstránkach a v reklamných kampaniach,
- neotvárajte podozrivé a nevyžiadané e-maily, nespúšťajte podozrivé a nevyžiadané prílohy,
- všímajte si skutočného odosielateľa správy a jej formálnu a obsahovú bezchybnosť,
- používajte a aktualizujte si antimalvér riešenie, ktoré obsahuje aj nástroje pre ochranu proti spamu,
- na mailovom serveri aktivujte filtrovanie pošty obsahujúcej spustiteľné súbory, prípadne súbory zodpovedajúce niektorým indikátorom nákazy,
- zálohujte dôležité súbory: ideálne na dve rôzne média, ktoré nie sú trvalo pripojené k zariadeniu a z ktorých jedno je uložené na bezpečnom mieste

Zdroje:
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=126