Mesačný prehľad kritických zraniteľností
December 2014

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2014-6363 skriptovacieho enginu VBScript spôsobená nesprávnou prácou s objektmi v pamäti počas zobrazovania využívajúceho renderovacie jadro Internet Explorer. Útočník môže zraniteľnosť zneužiť na vzdialené spustenie škodlivého kódu pomocou škodlivej web stránky alebo dokumentu Office využívajúceho zobrazenie pomocou InternetExplorera. Útočník získa oprávnenia užívateľa, ktorý infikovanú stránku zobrazil.

Zraniteľné systémy:

VBScript 5.6
VBScript 5.7
VBScript 5.8
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 x64-based Systems Service Pack 2
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 Itanium-based Systems Service Pack 1
Windows Server 2012
Windows Server 2012 R2

Odporúčania:

Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označeniami MS14-080 (pre systémy s Internet Explorer 9-11) a MS14-084 (pre systémy s Internet Explorer do verzie 8 alebo bez neho). Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú verejne dostupné a používané. Správcom systémov odporúčame prezrieť si decembrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroj:
https://technet.microsoft.com/library/security/ms14-080
https://technet.microsoft.com/library/security/ms14-084

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2014-6356 a CVE-2014-6357 spôsobené chybami pri práci s objektmi v pamäti (chybné indexovanie poľa a opätovné použitie uvoľnenej pamäte) pri spracovaní nekorektných dokumentov Microsoft Word. Zraniteľnosti umožňujú vzdialené spustenie škodlivého kódu po otvorení infikovaného dokumentu Microsoft Office Word.
Taktiež bol zaznamenaný zvýšený výskyt zneužívania makier v produktoch Microsoft Office a zvýšený výskyt podvodných e-mailov so škodlivými prílohami zneužívajúcimi tento spôsob útoku.

Zraniteľné systémy:
Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 (64-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2013 RT
Microsoft Office 2013 RT Service Pack 1
Microsoft Office for Mac 2011
Microsoft Word Viewer
Microsoft Office Compatibility Pack Service Pack 3
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2013
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps 2013
Microsoft Office Web Apps 2013 Service Pack 1

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS14-081. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú pravdepodobne používané.
Správcom systémov odporúčame prezrieť si decembrový Microsoft Security Bulletin dostupný na odkaze nižšie.
Používateľom odporúčame nepovoľovať makrá pre nedôveryhodné súbory a nespúšťať nepodpísané makrá v dokumentoch Microsoft Office. Taktiež odporúčame zvýšenú opatrnosť a neotvárať podozrivé a nevyžiadané e-maily a prílohy v nich.

Zdroje:
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=125
https://www.csirt.gov.sk/aktualne-7d7.html?id=80
https://technet.microsoft.com/library/security/ms14-081

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala pravidelnú kumulatívnu sadu záplat na zraniteľnosti, z ktorých najzávažnejšie umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky. Na mnohé z týchto zraniteľností je výskyt exploitov a ich použitie pravdepodobné.

Zraniteľné systémy:
Microsoft Internet Explorer 6-11

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS14-080. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú známe a používané. Správcom systémov odporúčame prezrieť si decembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/library/security/ms14-080

Mozilla Firefox

Spoločnosť Mozilla vydala novú verziu prehliadača Firefoxopravujúcu 9 zraniteľností, z toho tri kritické.
Zraniteľnosť CVE-2014-1593 spôsobená chybou typu buffer-overflow na zásobníku umožňujúca vzdialené spustenie škodlivého kódu pri spracovávaní mediálneho obsahu.
Zraniteľnosť CVE-2014-1592 spôsobená opätovným použitím uvoľnenej pamäte umožňujúca vzdialené spustenie škodlivého kódu pri spracovávaní HTML5 dokumentu.
Viaceré bližšie nešpecifikované zraniteľnosti pri práci s pamäťou umožňujúce útočníkovi spôsobiť pád aplikácie a možné spustenie škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 33 a predchádzajúce
Mozilla Firefox ESR 31.2 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé verzie na najnovšie verzie (Mozilla Firefox 34.0.5 a Mozilla Firefox ESR 31.3).

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/
https://www.mozilla.org/sk/security/advisories/mfsa2014-83/
https://www.mozilla.org/sk/security/advisories/mfsa2014-87/
https://www.mozilla.org/sk/security/advisories/mfsa2014-88/
https://www.mozilla.org/en-US/firefox/34.0.5/releasenotes/

Google Chrome

Spoločnosť Google vydala novú verziu prehliadača Chrome, ktorá obsahuje aktualizáciu prehrávača Adobe Flash opravujúcu viacero zraniteľností a tiež niekoľko ďalších opráv.

Zraniteľné systémy
Google Chrome do verzie 39.0.2171.95

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 39.0.2171.95. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2014/12/stable-channel-update.html

4. Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci december aktualizáciu opravujúcu 6 zraniteľností. Zraniteľnosti sú spôsobené prevažne rôznymi chybami pri práci s pamäťou a umožňujú vzdialenému útočníkovi spustenie škodlivého kódu a odhalenie citlivých informácií.

Zraniteľné systémy
Adobe Flash Player do verzie 15.0.0.242
Adobe Flash Player do verzie 13.0.0.258
Adobe Flash Player do verzie 11.2.202.424

Odporúčania:
Užívateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 16.0.0.235, užívateľom Adobe Flash Player s predĺženou podporou odporúčame aktualizovať na verziu 13.0.0.259. Užívateľom Linux odporúčame aktualizovať na verziu 11.2.202.425.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player 15.x.

Zdroje:
http://helpx.adobe.com/security/products/flash-player/apsb14-27.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci december nevydala žiadnu aktualizáciu frameworku Microsoft .NET.

Zdroje:
https://technet.microsoft.com/library/security/ms14-dec

Oracle Java

Spoločnosť Oracle nevydala v mesiaci december žiadnu aktualizáciu platformy Java. Najbližšia veľká sada aktualizácii je naplánovaná na 20. január 2015.

Zdroje:
http://www.oracle.com/technetwork/topics/security/alerts-086861.html

6. Iné závažné zraniteľnosti

Misfortune cookie

Spoločnosť Checkpoint zverejnila informáciu o objavenej chybe vo firmvéri malých domácich a kancelárskych smerovačov (SOHO router) s integrovaným webovým serverom RomPager. Webový server Rompager od spoločnosti Allegro používajú vo svojich zariadeniach mnohí výrobcovia, napr. ZyXEL, D-Link, TP-Link, Huawei, Asus.
Zraniteľnosť je zapríčinená spôsobom, akým RomPager spracováva cookies (statická alokácia pamäte pre 10 cookies o veľkosti 40 B). Útočník tak môže pomocou odoslania špeciálnej požiadavky s niekoľkými cookies obísť autentifikáciu vo webovom administračnom rozhraní smerovača a prevziať kontrolu nad zariadením.

Zraniteľné systémy:
RomPager do verzie 4.34
Zoznam zraniteľných zariadení nájdete na http://mis.fortunecook.ie/misfortune-cookie-suspected-vulnerable.pdf

Odporúčania:
Majiteľom zraniteľných smerovačov odporúčame skontrolovať dostupnosť aktualizácii firmvéru zariadenia na stránkach výrobcu. Na mnohé zariadenia však už výrobcovia nové

verzie firmvéru nevydávajú, a možnosti bežných užívateľov zraniteľných smerovačov sú v tomto prípade obmedzené. Pokročilí užívatelia majú ešte možnosť pokúsiť sa do smerovača nahrať alternatívny firmvér (OpenWrt, DD-WRT), pokiaľ to ich zariadenie umožňuje.

Odporúčania na zmiernenie rizika:

- Pokiaľ je to možné, odporúčame v konfiguračnom rozhraní smerovača zakázať prístup do routra z „vonku“ (cez WAN rozhranie) a pravidelne kontrolovať nastavenie DNS resolverov.
- Pokiaľ máte vo vašej sieti zapojený medzi zraniteľným smerovačom a internetom firewall, nakonfigurujte ho tak, aby blokoval všetky spojenia z prostredia Internetu na Váš smerovač.
- Ak nie je nič z vyššie uvedeného možné, odporúčame uvažovať o výmene smerovača.

Zdroje:
http://mis.fortunecook.ie/
http://mis.fortunecook.ie/too-many-cooks-exploiting-tr069_tal-oppenheim_31c3.pdf