Mesačný prehľad kritických zraniteľností
September 2015

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2015-2546 v Microsoft Windows kernel-mode driver (Win32k.sys) je spôsobená nesprávnym prístupom k objektom v pamäti, čo môže byť zneužité na zvýšenie oprávnení procesu až na systémovú úroveň. Bolo zaznamenané použitie exploitov na túto zraniteľnosť pri cielených útokoch.

Zraniteľnosť CVE-2015-2510 spôsobené chybami pri spracovaní OpenType fontov. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované OpenType fonty. Útočník zneužitím tejto zraniteľnosti môže získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľnosti CVE-2015-2513, CVE-2015-2519 a CVE-2015-2530 aplikácie Windows Denník sú spôsobené chybami pri spracovaní súborov Windows Denníka. Umožňujú vzdialené spustenie škodlivého kódu po otvorení infikovaného súboru.

Zraniteľnosť CVE-2015-2509 vo Windows Media Center pri spracovávaní súborov Media Center link umožňuje spustenie škodlivého kódu pomocou otvorenia .mcl súboru s odkazom na tento škodlivý program. Takto infikovaný .mcl súbor môže byť stiahnutý z webovej stránky alebo môže byť prílohou e-mailu. Exploit na túto zraniteľnosť je verejne dostupný.

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 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows RT
Windows RT 8.1
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 uvedené zraniteľnosti sú distribuované pod označeniami MS15-097, MS15-098 a MS15-100. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti sú verejne známe a použitie exploitov na ostatné zraniteľnosti je pravdepodobné.
Správcom systémov odporúčame prezrieť si septembrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms15-097.aspx
https://technet.microsoft.com/en-us/library/security/ms15-098.aspx
https://technet.microsoft.com/en-us/library/security/ms15-100.aspx
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=139
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=141

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2015-2545 v Microsoft Office pri spracovávaní infikovaného grafického objektu vo formáte EPS. Otvorenie dokumentu s infikovaným obrázkom alebo vloženie takéhoto obrázka do dokumentu môže byť zneužité na vzdialené spustenie škodlivého kódu. Bolo zaznamenané použitie exploitov na túto zraniteľnosť pri cielených útokoch.

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 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2016 (32-bit editions)
Microsoft Office 2016 (64-bit editions)

Microsoft Excel for Mac 2011
Microsoft Excel for Mac 2016
Microsoft Excel Viewer
Microsoft Office Compatibility Pack Service Pack 3

Microsoft SharePoint Foundation 2013 Service Pack 1

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením

MS15-099. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitov na zraniteľnosť CVE-2015-2545.
Správcom systémov odporúčame prezrieť si septembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms15-099.aspx
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=139

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala jednu sadu záplat na 17 zraniteľnosti, z ktorých 13 je označených ako kritických, sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľné systémy:
Microsoft Internet Explorer 7
Microsoft Internet Explorer 8
Microsoft Internet Explorer 9
Microsoft Internet Explorer 10
Microsoft Internet Explorer 11

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-094. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si septembrové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms15-094.aspx

Microsoft Edge

Spoločnosť Microsoft vydala jednu sadu záplat na 4 zraniteľnosti, z ktorých sú všetky označené ako kritické, sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľné systémy:
Microsoft Edge

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením

MS15-095. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si septembrové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms15-095.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci september jednu aktualizáciu prehliadača Firefox opravujúce 6 kritických zraniteľností.

Zraniteľnosti CVE-2015-7178 a CVE-2015-7179 v grafickej knižnici ANGLE sú spôsobené pretečením pamäte (buffer overflow) a zápisom mimo pridelenej pamäte. Obe zraniteľnosti umožňujú vzdialené spustenie škodlivého kódu pri spracovaní OpenGL, resp. WebGL obsahu.

Zraniteľnosť CVE-2015-4509 v rozhraní pre HTML Video element spôsobená opätovným použitím uvoľnenej pamäte umožňuje vzdialené spustenie škodlivého kódu prostredníctvom JavaScript kódu manipulujúceho s elementom.

Zraniteľnosť CVE-2015-4510 spôsobená opätovným použitím uvoľnenej pamäte počas behu viacerých vlákien pristupujúcich k IndexedDB umožňuje vzdialené spustenie škodlivého kódu pri interakcii vlákien a IndexedDB.

Zraniteľnosti CVE-2015-4500, CVE-2015-4501 spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 40.0.3 a predchádzajúce
Mozilla Firefox ESR 38.2.1 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 41 a Mozilla Firefox ESR 38.3)
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/

Google Chrome

Spoločnosť Google štyri aktualizácie prehliadača Chrome, ktoré obsahujú opravy bezpečnostných zraniteľností aj novú verziu Adobe Flash Player.

Okrem zraniteľností, ktoré sme uvádzali v minulom mesačníku, sú najvážnejšie opravené zraniteľnosti CVE-2015-1303 a CVE-2015-1304 umožňujú spôsobiť obísť zabezpečenie Same-origin-policy (Cross-origin bypass).

Zraniteľné systémy
Google Chrome do verzie 45.0.2454.101

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 45.0.2454.101. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2015/09/stable-channel-update_24.html
http://googlechromereleases.blogspot.in/2015/09/stable-channel-refresh.html
http://googlechromereleases.blogspot.in/2015/09/stable-channel-update_15.html
http://googlechromereleases.blogspot.in/2015/09/stable-channel-update.html
http://www.csirt.gov.sk/doc/2015_08_mesacnik.pdf

4. Adobe Flash Player

Spoločnosť Adobe vydala aktualizáciu opravujúcu 23 zraniteľnosti, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené opätovným použitím uvoľnenej pamäte, pretečením pamäte a zásobníka (buffer overflow, stack overflow), pretečením použitím nesprávnych typov premenných a ďalšími chybami pri práci s pamäťou. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód pomocou infikovaného Flash obsahu.

Zraniteľné systémy
Adobe Flash Player verzie 18.0.0.232 a nižšej
Adobe Flash Player verzie 11.2.202.508 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 19.0.0.185, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.241. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.508.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb15-23.html

5. Frameworky

Microsoft .NET Framework

Zraniteľnosť CVE-2015-2504 spôsobená chybou pri kopírovaní objektov v pamäti umožňuje zvýšenie oprávnení procesu. Zraniteľnosť môže byť zneužitá navštívením webstránky, ktorá obsahuje XAML aplikáciu bežiacu v prehliadači alebo spustením .NET aplikácie. Útočník zneužitím tejto zraniteľnosti môže získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľné systémy
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5/3.5.1
Microsoft .NET Framework 4
Microsoft .NET Framework 4.5/4.5.1/4.5.2
Microsoft .NET Framework 4.6

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-101. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si septembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms15-101.aspx

Oracle Java

Spoločnosť Oracle v mesiaci jún nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 20. október 2015.

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

6. Iné závažné zraniteľnosti

Android Stagefright

Na Internete bol zverejnený exploit zneužívajúci zraniteľnosť Stagefright v mobilnom operačnom systéme Android. Útočníci môžu zneužiť uvedený exploit na vytvorenie infikovaného súboru vo formáte MP4, ktorý po odoslaní na zraniteľné zariadenie otvorí útočníkom do systému obete zadné dvierka, prostredníctvom ktorých môžu prevziať kontrolu nad napadnutým zariadením. Exploit je verejne dostupný pre testovacie a vzdelávacie účely, ale jeho zneužitie nevyžaduje veľkú mieru technických znalostí.
Zraniteľnostiam Stagefright sme sa venovali v júlovom mesačníku.

Zraniteľné systémy:
Android 2.2 a novší

Odporúčania:
Používateľom odporúčame aplikovať najnovšie dostupné aktualizácie pre ich zariadenia. Ďalej odporúčame používateľom zraniteľných zariadení zablokovať automatické sťahovanie multimediálnych správ (napr. MMS, Hangouts), resp. ich príloh, prípadne zablokovať prijímanie MMS od neznámych čísel, ak to daná aplikácia umožňuje. V prípade ak takáto možnosť neexistuje, odporúčame aplikáciu odinštalovať. Odporúčame zvážiť aj možnosť úplného zablokovania prístupu na Internet a prijímania MMS správ v nastaveniach mobilného zariadenia.

Ďalšou možnosťou je nainštalovať si alternatívnu aplikáciu pre multimediálne správy. Avšak treba brať ohľad na dôveryhodnosť inštalovanej aplikácie a zdroja, z ktorého pochádza. Útočníci môže využiť vzniknutú situáciu vydávaním podvodných a infikovaných aplikácií pre multimediálne správy.

Zdroje:
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=140
http://www.csirt.gov.sk/doc/2015_07_mesacnik.pdf

Android Stagefright 2.0

Boli zverejnené čiastočné informácie o ďalších dvoch zraniteľnostiach CVE-2015-6602 a CVE-2015-3876 knižnice libutils a multimediálnej knižnice libstagefright, ktoré vzdialenému útočníkovi umožňujú prevziať kontrolu nad zariadením po otvorení webstránky obsahujúcej infikovaný multimediálny obsah.

Zraniteľné systémy:
Android 1.0 a novší

Odporúčania:
Používateľom odporúčame navštevovať iba dôveryhodné stránky a neklikať na odkazy v e-mailoch pochádzajúcich z nedôveryhodných zdrojov. Taktiež odporúčame zvážiť možnosť úplného zablokovania prístupu na Internet.

Zdroje:
https://blog.zimperium.com/zimperium-zlabs-is-raising-the-volume-new-vulnerability-processing-mp3mp4-media/

TrueCrypt

Zraniteľnosti CVE-2015-7358 a CVE-2015-7359 v ovládači šifrovacieho programu TrueCrypt spôsobené nesprávnou kontrolou symbolických odkazov umožňujú manipulovanie s diskami iných užívateľov a zvýšenie oprávnení.

Zraniteľné systémy:
TrueCrypt

Odporúčania:
Nakoľko vývoj programu TrueCrypt bol zastavený, tieto zraniteľnosti nebudú opravené. Riešením pre používateľov programu TrueCrypt môže byť prejdenie na alternatívny softvér, ktorý tieto zraniteľnosti už má opravené, napr. VeraCrypt.

Zdroje:
http://www.itworld.com/article/2987438/data-protection/newly-found-truecrypt-flaw-allows-full-system-compromise.html
https://veracrypt.codeplex.com/wikipage?title=Release%20Notes

SYNful Knock - Kompromitované smerovače Cisco

Spoločnosť FireEye publikovala informácie o kompromitácii smerovačov (routerov) spoločnosti Cisco.
Na základe doterajších zistení útočníci pravdepodobne získali prístup do zariadení pomocou uhádnutých alebo ukradnutých administrátorských hesiel a následne modifikovali operačný systém IOS používaný v smerovačoch a prepínačoch firmy Cisco.

Modifikácia IOS pozostáva z prepísania niektoré časti pôvodného IOS prepísané malvérom a umožňuje útočníkovi načítať rôzne moduly pre rozšírenie funkcionality. Útočník môže spravovať načítané moduly na diaľku z prostredia Internetu po odoslaní špeciálnej sekvencie TCP packetov slúžiacich pre aktivovanie vzdialenej správy tohto malvéru (odtiaľ názov SYNful Knock).
Napadnuté zariadenie taktiež obsahuje zadné dvierka pre útočníka. Zadné dvierka sú prístupné prostredníctvom Telnetu alebo konzoly po zadaní backdoor hesla cez protokol HTTP. Útočník má pri použití zadných dvierok neobmedzené systémové oprávnenia a môže napr. odchytiť, presmerovať alebo modifikovať komunikáciu.

Odporúčania:
Odporúčame preveriť kompromitáciu Cisco smerovačov niektorou z metód uvedených v odkazoch nižšie. Po potvrdení kompromitácie odporúčame preinštalovať zariadenie pomocou čistého obrazu IOS priamo od spoločnosti Cisco a následne overiť kontrolné súčty nainštalovaného a stiahnutého obrazu.
Ďalej odporúčame zabezpečiť smerovač na základe odporúčaní spoločnosti Cisco dostupných na adrese http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html.
V prípade zistenej kompromitácie smerovača taktiež odporúčame skontrolovať ostatné zariadenia v sieti na prítomnosť škodlivého kódu a po vyčistení a zabezpečení smerovača dôkladne sledovať komunikáciu v sieti a vyhľadávať anomálie, ktoré môžu viesť k odhaleniu pokusom o novú kompromitáciu smerovača.

Referencie:
https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html
https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis0.html