Mesačný prehľad kritických zraniteľností
Júl 2015

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2015-2372 skriptovacieho enginu VBScript počas zobrazovania v Internet Explorer je spôsobená nesprávnou prácou s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení infikovanej webstránky alebo dokumentu Office využívajúceho Internet Explorer. Útočník získa rovnaké práva ako užívateľ, ktorý škodlivý obsah zobrazil.

Zraniteľnosť CVE-2015-2373 vo Windows službe RDP (Remote Desktop Protocol) spôsobená nesprávnou chybou pri spracovaní packetov. Vzdialený útočník môže odoslaním série škodlivých packetov spôsobiť pád služby RDP, prípadne spustiť ľubovoľný kód so systémovými právami a prevziať kontrolu nad zariadením.

Zraniteľnosť CVE-2015-2361 vo virtualizačnej technológii Hyper-V je spôsobená nesprávnou inicializáciou pamäte na základe veľkosti packetov vo virtuálnom počítači, čo umožňuje spôsobiť pretečenie pamäte (buffer overflow).
Zraniteľnosť CVE-2015-2362 vo virtualizačnej technológii Hyper-V je spôsobená nesprávnou inicializáciou systémových dátových štruktúr vo virtuálnom počítači.
Obe tieto zraniteľnosti umožňujú útočníkovi prihlásenému na virtuálnom počítači s oprávneniami administrátora spustiť škodlivý kód na hostiteľskom zariadení.

Zraniteľnosť CVE-2015-2387 v knižnici Adobe Type Manager (ATMFD.dll) spôsobená chybou pri práci s objektami v pamäti. Útočník prihlásený do systému ako normálny užívateľ môže zneužitím tejto zraniteľnosti prostredníctvom spustenia škodlivého programu zvýšiť svoje oprávnenia na úroveň administrátora. Exploit na túto zraniteľnosť je verejne známy.

Zraniteľnosť CVE-2015-2426 v knižnici Adobe Type Manager spôsobená chybou pri spracovávaní OpenType fontov. Umožňuje 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.

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 10 for 32-bit Systems
Windows 10 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 uvedené zraniteľnosti sú distribuované pod označeniami MS15-066, MS15-067, MS15-068, MS15-077 a MS15-078. 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 júlové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-066
https://technet.microsoft.com/library/security/MS15-067
https://technet.microsoft.com/library/security/MS15-068
https://technet.microsoft.com/library/security/MS15-077
https://technet.microsoft.com/library/security/MS15-078

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2015-2376, CVE-2015-2377, CVE-2015-2379, CVE-2015-2380, CVE-2015-2415 a CVE-2015-2424 spôsobené chybami pri práci s objektmi v pamäti umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor. Bolo zaznamenané použitie exploitov na zraniteľnosť CVE-2015-2424.

Zraniteľnosť CVE-2015-2378 v aplikácii Microsoft Excel spôsobená chybou pri načítavaní dynamicky linkovaných knižníc (.dll). Útočník, ktorý umiestni do aktuálneho pracovného adresára užívateľa infikovaný .dll súbor, môže následne zneužiť túto zraniteľnosť na spustenie škodlivého kódu so systémovými oprávneniami a prevziať tak kontrolu nad napadnutým zariadením.

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 for Mac 2011
Microsoft Word Viewer
Microsoft Excel Viewer 2007 Service Pack 3
Microsoft Office Compatibility Pack Service Pack 3

Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions)
Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions)
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2013 Service Pack 1

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-070. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitov na zraniteľnosť CVE-2015-2424.
Správcom systémov odporúčame prezrieť si júlový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-070

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na zraniteľnosti, z ktorých 21 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 6

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 MS15-065. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitu na zraniteľnosť CVE-2015-2425 a výskyt exploitov na niektoré iné zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si júlový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/library/security/MS15-065

Microsoft Internet Explorer Mobile

Spoločnosť TippingPoint prostredníctvom programu ZDI (Zero Day Initiative) zverejnila informácie o štyroch 0-day zraniteľnostiach prehliadača Microsoft Internet Explorer pre smartfóny. Tri z nich sú spôsobené opätovným použitím uvoľnenej pamäte. Štvrtá zraniteľnosť je spôsobená použitím pamäte za koncom poľa buniek pri práci s HTML tabuľkami. Všetky štyri zraniteľnosti umožňujú vzdialené spustenie škodlivého kódu s oprávneniami procesu prehliadača po navštívení infikovanej webstránky.

Zraniteľné systémy:
Microsoft Internet Explorer Mobile

Zdroj:
http://www.zerodayinitiative.com/advisories/ZDI-15-359/
http://www.zerodayinitiative.com/advisories/ZDI-15-360/
http://www.zerodayinitiative.com/advisories/ZDI-15-361/
http://www.zerodayinitiative.com/advisories/ZDI-15-362/

Odporúčania:
Spoločnosť Microsoft zatiaľ nezverejnila opravy uvedených zraniteľností. Na zmiernenie rizika odporúčame nepoužívať Microsoft Internet Explorer Mobile, prípadne vypnúť Active Scripting.

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci júl jednu aktualizáciu prehliadača Firefox opravujúcu 22 zraniteľností, z toho je 13 označených ako kritických. Zároveň boli opravené chyby súvisiace s Logjam útokom (http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=134)

Zraniteľnosti CVE-2015-2735 a CVE-2015-2736 spôsobené prístupom k nesprávnej pamäti umožňujú spôsobiť bližšie neurčené dôsledky prostredníctvom škodlivého ZIP archívu.

Zraniteľnosti CVE-2015-2734, CVE-2015-2737, CVE-2015-2738 a CVE-2015-2739 spôsobené čítaním z neinicializovanej pamäte, resp. prístupom k nesprávnej pamäti umožňujú spôsobiť bližšie neurčené dôsledky prostredníctvom bližšie neurčeného spôsobu.

Zraniteľnosť CVE-2015-2740 spôsobená pretečením pamäte (buffer overflow) umožňuje spôsobiť pád aplikácie, prípadne spustenie škodlivého kódu prostredníctvom bližšie neurčeného spôsobu.

Zraniteľnosti CVE-2015-2722 a CVE-2015-2733 spôsobená opätovným použitím uvoľnenej pamäte umožňujú vzdialené spustenie škodlivého kódu prostredníctvom XMLHttpRequest.

Zraniteľnosť CVE-2015-2731 spôsobená opätovným použitím uvoľnenej pamäte pri odstránení DOM objektu na základe Content Policy umožňuje vzdialené spustenie škodlivého kódu.

Zraniteľnosti CVE-2015-2724, CVE-2015-2725 a CVE-2015-2726 spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 38 a predchádzajúce
Mozilla Firefox ESR 31.7 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 39 a Mozilla Firefox ESR 31.8)
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 päť aktualizácií prehliadača Chrome, ktoré obsahujú opravy 43 bezpečnostných zraniteľností a taktiež obsahujú novú verziu Adobe Flash Player.

Najvážnejšie zraniteľnosti sú spôsobené najmä chybami pri práci s pamäťou (zápis mimo hraníc, znovupoužitie uvoľnenej pamäte) a umožňujú spôsobiť pád aplikácie, prípadne vložiť JavaScript alebo HTML kód do zobrazenej stránky (Cross-site scripting).

Zraniteľné systémy
Google Chrome do verzie 44.0.2403.89

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 44.0.2403.89, resp. 44.0.2403.130, nakoľko exploity na niektoré zraniteľnosti Flash Playera sú už používané a verejne známe. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2015/07/stable-channel-update.html
http://googlechromereleases.blogspot.in/2015/07/stable-channel-update_14.html
http://googlechromereleases.blogspot.in/2015/07/stable-channel-update_21.html
http://googlechromereleases.blogspot.in/2015/07/stable-channel-update_24.html
http://googlechromereleases.blogspot.in/2015/07/stable-channel-update_28.html

4. Adobe Flash Player

Spoločnosť Adobe vydala aktualizáciu opravujúcu 2 zraniteľnosti, z toho obe sú označené ako kritické.

Zraniteľnosti CVE-2015-5122 a CVE-2015-5123 spôsobené opätovným použitím uvoľnenej pamäti umožňuje vzdialenému útočníkovi spustiť škodlivý kód pomocou infikovaného Flash obsahu. Exploity na obe zraniteľnosti sú verejne dostupné a intenzívne používané pri útokoch.

Zraniteľné systémy
Adobe Flash Player verzie 18.0.0.203 a nižšej
Adobe Flash Player verzie 13.0.0.302 a nižšej
Adobe Flash Player verzie 11.2.202.481 a nižšej

Odporúčania:
Užívateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 18.0.0.209, užívateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu

13.0.0.309. Užívateľom Linux odporúčame aktualizovať na verziu 11.2.202.491. Aktualizáciu odporúčame vykonať čo najskôr, nakoľko exploity na obe zraniteľnosti sú verejne známe a používané.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player 18.x.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb15-18.html
https://www.fireeye.com/blog/threat-research/2015/07/cve-2015-5122_-_seco.html
http://www.symantec.com/connect/blogs/third-adobe-flash-zero-day-exploit-cve-2015-5123-leaked-hacking-team-cache

5. Frameworky

Microsoft .NET Framework

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

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

Oracle Java

Spoločnosť Oracle v mesiaci júl vydala bezpečnostnú aktualizáciu platformy Java obsahujúcu 25 zraniteľností, z ktorých je 10 závažných.

Zraniteľnosti CVE-2015-4760, CVE-2015-2628, CVE-2015-4731, CVE-2015-2590, CVE-2015-4732, CVE-2015-4733, CVE-2015-2638, CVE-2015-4736, CVE-2015-4748 a CVE-2015-2597 umožňujú vzdialenému, prípadne lokálnemu užívateľovi bez autentifikácie spustenie škodlivého kódu, prípadne kompromitáciu zariadenia. Exploity na niektoré zraniteľnosti už boli zaznanenané (CVE-2015-2590) a sú používané pri útokoch.

Zraniteľné systémy:
Java SE 6u95
Java SE 7u80
Java SE 8u45

Odporúčania:
Spoločnosť Oracle zverejnila aktualizáciu prostredníctvom bežného kanála Java Auto Update. Aktualizácie sú dostupné aj na stránke java.com. Používateľom odporúčame nainštalovať najnovšiu verziu Java SE 8 Update 51.

Zdroje:
http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-trend-micro-discovers-new-java-zero-day-exploit/

6. Iné závažné zraniteľnosti

VMware host privilege escalation

Zraniteľnosť CVE-2015-3650 spôsobená nesprávnym ukazovateľom na DACL (discretionary access controll list) štruktúru v procese vprintproxy.exe umožňujúca lokálnemu užívateľovi hostiteľského systému získať systémové oprávnenia hostiteľského systému.

Zraniteľné systémy:
VMware Workstation 11.x do verzie 11.1.1
VMware Workstation 7.x-10.x do verzie 10.0.7
VMware Player 7.x do verzie 7.1.1
VMware Player 5.x a 6.x do verzie 6.0.7
VMware Horizon Client 5.x do verzie 5.4.2

Odporúčania:
Spoločnosť VMware zverejnila aktualizácie na svojich stránkach. Odporúčame aktualizovať zraniteľné produkty na najnovšie verzie.

Zdroje:
http://www.vmware.com/security/advisories/VMSA-2015-0005

Stagefright

Zraniteľnosť zariadení so systémom Android, ktorá umožňuje vzdialené spustenie škodlivého kódu prostredníctvom MMS obsahujúcej infikované video. Zraniteľnosť spočíva v spôsobe, akým Android spracováva video obsah. V niektorých prípadoch teda stačí na úspešné napadnutie zariadenia iba prijatie alebo náhľad MMS správy bez jej otvorenia. Odhaduje sa, že touto zraniteľnosťou trpí 95% zariadení s Androidom. Najviac rizikové sú zariadenia s Androidom 2.2 Froyo a 2.3 Gingerbread, pretože pre ne existuje viacero spôsobov, ako získať práva roota (administrátorské práva) a následne prevziať kontrolu nad celým zariadením.

Zraniteľné systémy:
Android 2.2 a novší

Odporúčania:

Spoločnosť Google síce vydala aktualizáciu opravujúcu túto zraniteľnosť, ale jej adaptovanie všetkými výrobcami zraniteľných zariadení sa zatiaľ neuskutočnilo, a pravdepodobne sa ani neuskutoční, nakoľko mnohé zariadenia a staršie verzie OS Android už podporované nie sú. Užívateľom zraniteľných zariadení na zmiernenie rizika odporúčame zablokovať automatické sťahovanie MMS, resp. ich príloh, prípadne zablokovať prijímanie MMS od neznámych čísel, ak to daná aplikácia dovoľuje. Pokiaľ sa však užívatelia rozhodnú nainštalovať si alternatívnu MMS aplikáciu, treba brať ohľad na dôveryhodnosť aplikácie, nakoľko takáto aplikácia bude mať prístup k správam užívateľa.

Zdroje:

https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/
https://blog.zimperium.com/how-to-protect-from-stagefright-vulnerability/