Mesačný prehľad kritických zraniteľností
Máj 2015

1. Operačné systémy Microsoft Windows

Zraniteľnosti CVE-2015-1675, CVE-2015-1695 až CVE-2015-1699 aplikácie pre tvorbu poznámok Windows Journal (Windows Denník) umožňujú spustenie škodlivého kódu po otvorení .jnt súboru v aplikácii. Vzdialený útočník môže túto zraniteľnosť zneužiť prostredníctvom e-mailov s infikovanou prílohou, ak užívateľ prílohu otvorí. Dve zraniteľnosti boli publikované verejne a je pravdepodobné ich zneužitie.

Zraniteľnosť CVE-2015-1701 vo Windows kernel-mode driver (Win32k.sys) spôsobená nesprávnou prácou s objektmi v pamäti. Útočník prihlásený do systému môže zneužiť túto zraniteľnosť na spustenie programov so systémovými právami a prevziať kontrolu nad zariadením. Táto zraniteľnosť bola publikovaná verejne a boli zaznamenané jej zneužitia v kombinácii s exploitom pre Flash player na vzdialené spustenie škodlivého kódu so systémovými právami.

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 x6k4-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 uvedené zraniteľnosti sú distribuované pod označeniami MS15-045, MS15-050, MS15-051. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú používané pri útokoch. Správcom systémov odporúčame prezrieť si marcové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Ak aplikáciu Windows Denník nepoužívate, odporúčame ju odstrániť zo systému Microsoft Windows pomocou nasledovného postupu:

1) Štart -> Ovládací panel -> Programy a súčasti
2) Zapnúť alebo vypnúť súčasti systémy Windows -> odškrtnúť Súčasti počítača Tablet PC
3) Potvrdiť OK

Zdroje:

https://technet.microsoft.com/library/security/MS15-045
https://technet.microsoft.com/library/security/MS15-051

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2015-1682 a CVE-2015-1683 spôsobené chybami pri práci s objektmi v pamäti počas spracovania dokumentov Office umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor.

Zraniteľnosť CVE-2015-1671 knižnice Windows DirectWrite spôsobená nesprávnym spracovaním TrueType fontov umožňuje útočníkovi vzdialené spustenie škodlivého kódu so systémovými oprávneniami po otvorení infikovaného súbora alebo navštívení webovej stránky obsahujúcej TrueType fonty. Útočník môže následne prevziať kontrolu nad systémom obete.

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 PowerPoint Viewer
Microsoft Excel Viewer
Microsoft Office Compatibility Pack Service Pack 3
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft Office Web Apps 2010 Service Pack 2
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 označeniami MS15-044 a MS15-046. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitov na zraniteľnosť
CVE-2015-1671.
Pokiaľ používate produkty Microsoft Office 2013, odporúčame prejsť na produkty 2013 Service Pack 1, pretože pôvodné verzie už nie sú ďalej podporované.
Správcom systémov odporúčame prezrieť si májové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-044
https://technet.microsoft.com/library/security/MS15-046
https://support.microsoft.com/sk-sk/lifecycle?p1=16674

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na zraniteľnosti, z ktorých 14 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 - 11

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-043. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si aprílový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/library/security/MS15-043

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci máj jednu aktualizáciu prehliadača Firefox opravujúcu 13 zraniteľností, z toho je 5 označených ako kritických.

Zraniteľnosť CVE-2015-2716 spôsobená pretečením pamäte pri práci s veľkým množstvom komprimovaných XML údajov umožňuje vzdialené spustenie škodlivého kódu alebo spôsobiť pádu aplikácie.

Zraniteľnosť CVE-2015-2713 spôsobená opätovným použitím uvoľnenej pamäte pri práci s vertikálnym textom umožňuje vzdialené spustenie škodlivého kódu alebo spôsobiť pád aplikácie.

Zraniteľnosť CVE-2015-2712 spôsobená čítaním a zápisom mimo hraníc v asm.js pri kontrole JavaScriptového kódu umožňuje vzdialené spustenie škodlivého kódu alebo prečítanie časti pamäte, ktorá môže obsahovať citlivé údaje.

Zraniteľnosť CVE-2015-2710 spôsobená pretečením pamäte pri práci s obrázkom SVG využívajúcom špecifické CSS vlastnosti umožňuje vzdialené spustenie škodlivého kódu.

Zraniteľnosti CVE-2015-2708 a CVE-2015-2709 spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou umožňujú vzdialené spustenie škodlivého kódu alebo spôsobiť pád aplikácie.

Zraniteľné systémy:

Mozilla Firefox 37 a predchádzajúce

Mozilla Firefox ESR 31.6 a predchádzajúce

Odporúčania:

Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 38.0.1 a Mozilla Firefox ESR 31.7).

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 tri aktualizácie prehliadača Chrome, ktoré obsahujú opravy 37 bezpečnostných zraniteľností a taktiež obsahujú novú verziu Adobe Flash Player.

Najvážnejšia zraniteľnosť CVE-2015-1252 umožňuje obísť zabezpečenie sandbox pri práci s veľkým množstvom údajov.

Ďalšie vážne zraniteľnosti sú spôsobené najmä chybami pri práci s pamäťou (zápis mimo hraníc, znovu použitie uvoľnenej pamäte) a umožňujú obísť bezpečnostné mechanizmy (cross-origin).

Zraniteľné systémy:

Google Chrome do verzie 43.0.2357.65

Odporúčania:

Odporúčame aktualizovať prehliadač na verziu 43.0.2357.65, resp. 43.0.2357.81, nakoľko exploit na niektoré zraniteľnosti Flash Playera už je používaný. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:

http://googlechromereleases.blogspot.in/2015/05/stable-channel-update.html
http://googlechromereleases.blogspot.in/2015/05/stable-channel-update_19.html
http://googlechromereleases.blogspot.in/2015/05/stable-channel-update_25.html

4. Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci marec aktualizáciu opravujúcu 18 zraniteľností. Väčšina zraniteľnosti je spôsobená rôznymi chybami pri práci s pamäťou. Zraniteľnosti umožňujú vzdialenému útočníkovi spustenie škodlivého kódu alebo obídenie bezpečnostných prvkov (ASLR, chránený mód v Microsoft Internet Explorer). Na zraniteľnosť CVE-2015-3090 bol koncom mája zaznamenaný exploit využívajúci súbeh viacerých vlákien (race condition) počas úpravy rozmerov grafických objektov a práce s nimi. Tento exploit je súčasťou Angler Exploit Kitu, ktorý je v súčasnosti pravdepodobne najsofistikovanejším exploit kitom používaným pri kybernetickej trestnej činnosti.

Zraniteľné systémy

Adobe Flash Player verzie 17.0.0.169 a nižšej
Adobe Flash Player verzie 13.0.0.281 a nižšej
Adobe Flash Player verzie 11.2.202.457 a nižšej

Odporúčania:
Užívateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 17.0.0.188, užívateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 13.0.0.289. Užívateľom Linux odporúčame aktualizovať na verziu 11.2.202.460. 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 17.x.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb15-09.html
https://www.fireeye.com/blog/threat-research/2015/05/angler_ek_exploiting.html

5. Frameworky

Microsoft .NET Framework

Zraniteľnosť CVE-2015-1671 knižnice Windows DirectWrite spôsobená nesprávnym spracovaním TrueType fontov umožňuje útočníkovi vzdialené spustenie škodlivého kódu so systémovými oprávneniami po otvorení infikovaného súboru alebo navštívení webovej stránky obsahujúcej TrueType fonty. Útočník môže následne prevziať kontrolu nad systémom obete.

Zraniteľné systémy
Microsoft .NET Framework 3.0 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

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedenú zraniteľnosť sú distribuované pod označením MS15-044. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitov na uvedenú zraniteľnosť.
Správcom systémov odporúčame prezrieť si májový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-044

Oracle Java

Spoločnosť Oracle v mesiaci máj nevydala žiadne aktualizácie na platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 14. júl 2015.

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

6. Iné závažné zraniteľnosti

Venom

Zraniteľnosť CVE-2015-3456 je spôsobená pretečením pamäte (buffer overflow) v ovládači disketovej mechaniky virtualizačného nástroja QEMU. Útočník s lokálnym prístupom k disketovej jednotke vo virtualizovanom operačnom systéme môže zneužiť túto zraniteľnosť na spustenie škodlivého kódu v hostovanom systéme s rovnakými právami, aké má proces virtualizačného nástroja.
Zraniteľnosť Venom v projekte QEMU existuje od roku 2004.
Kód ovládača disketovej mechaniky z QEMU je použitý vo viacerých virtualizačných nástrojoch, ktoré sú preto tiež zraniteľné.

Zraniteľné systémy:
QEMU
Xen
KVM
VirtaulBox
Oracle VM

Hypervízory VMware, Microsoft Hyper-V a Bochs zraniteľné nie sú.

Odporúčania:
Pokiaľ používate niektorý z uvedených zraniteľných hypervízorov, odporúčame jeho aktualizáciu na najnovšiu verziu, nakoľko výrobcovia už vydali záplaty na zraniteľnosť Venom.

Zdroje:
http://venom.crowdstrike.com/
http://www.oracle.com/technetwork/topics/security/alert-cve-2015-3456-2542656.html

Logjam útok

Logjam je útok na zraniteľnosť v TLS protokole, pomocou ktorého môže útočník pri Man in the middle (MITM) útoku vynútiť použitie slabších kľúčov a po ich vypočítaní môže čítať a modifikovať šifrovanú komunkáciu.
Šifrovanie s použitím kratších kľúčov je možné z dôvodu podpory tzv. exportných šifrovacích sád, ktoré predstavujú zámerne oslabené verzie šifier určených na export mimo USA. Pri použití šifrovacej sady s Diffie-Hellmanovou výmenou dočasných kľúčov (DHE) môže MITM útočník vynútiť použitie exportnej sady (DHE_EXPORT), ktorá využíva kľúče dlhé nanajvýš 512 bitov.

Logjam útok je podobný útoku FREAK z marca 2015, avšak Logjam je skôr útokom na samotný TLS protokol a šifrovacie sady DHE, kým FREAK bol útokom na implementácie a šifrovacie sady RSA.
Pri Diffie-Hellmanovej výmene kľúčov je jedným z parametrov aj prvočíslo, ktoré sa používa pri výpočtoch kľúčov, no mnoho serverov v predvolenom nastavení používa vždy rovnaké prvočíslo. Pomocou vhodného predvypočítania niektorých hodnôt závisiacich na tomto prvočísle je možné odhaliť samotné kľúče takmer v reálnom čase a následne dešifrovať TLS komunikáciu.

Zraniteľné systémy:

Uvedená zraniteľnosť sa týka väčšiny moderných prehliadačov vrátane Google Chrome, Mozilla Firefox, Internet Explorer a Safari. Rovnako sa týka aj mnohých služieb využívajúcich protokol TLS, prípadne DH výmenu kľúčov, vrátane webových a mailových serverov, SSH a VPN, ktoré v predvolenom nastavení používajú niektoré z bežných prvočísel alebo dovoľujú použiť exportnú šifrovaciu sadu (DHE_EXPORT).
Zraniteľnosť vášho internetového prehliadača si môžete overiť na stránke https://weakdh.org/.
Zraniteľnosť serverov je možné overiť na stránke https://weakdh.org/sysadmin.html.

Odporúčania:

Odporúčame pravidelne a často kontrolovať dostupnosť aktualizácií prehliadačov. Hlavní výrobcovia prehliadačov plánujú čo najskôr vydať opravy prehliadačov, ktoré zakážu použitie krátkych kľúčov.
Správcom serverov odporúčame podporu exportných šifrovacíc sád vypnúť. Ak je to možné, odporúčame povoliť a preferovať použitie DH výmeny kľúčov založenej na eliptických krivkách ECDHE namiesto DHE, ktorá je v súčasnosti najodolnejšia voči známym útokom a pre ktorú nie je útok pomocou predvypočítaných hodnôt taký efektívny. Pri použití DHE odporúčame vygenerovať pre každú službu vlastné prvočíslo dlhé aspoň 2048 bitov.
Správcom serverom taktiež doporučujeme prečítať si odporúčané nastavenia pre serverové produkty Apache HTTP server, nginx, Microsoft IIS, Lighttpd, Apache Tomcat, Postfix SMTP, Sendmail, Dovecot, HAProxy a OpenSSH dostupné na stránke https://weakdh.org/sysadmin.html.

Zdroje:

https://weakdh.org/
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=134