Mesačný prehľad kritických zraniteľností
Marec 2015

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2015-0032 skriptovacieho enginu VBScript počas zobrazovania využívajúceho renderovacie jadro Internet Explorer je spôsobená nesprávnou prácou s objektmi v pamäti. Útočník môže zraniteľnosť zneužiť na vzdialené spustenie škodlivého kódu pomocou škodlivej webstránky alebo dokumentu Office využívajúceho Internet Explorer. Útočník získa oprávnenia užívateľa, ktorý infikovanú stránku zobrazil.

Zraniteľnosť CVE-2015-0081 Windows Text Services spôsobená nesprávnou prácou s objektmi v pamäti umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý zobrazí infikovanú stránku alebo otvorí infikovaný súbor.

Zraniteľnosť CVE-2015-0096 spôsobená chybou MS Windows pri načítavaní dynamických knižníc DLL umožňuje útočníkovi vzdialené spustenie škodlivého kódu a prevzatie kontroly nad systémom s oprávneniami užívateľa. Chybu je možné zneužiť pri zobrazení ikony infikovaných odkazov (zástupcov) pomocou Windows Explorer.

Zraniteľnosti CVE-2015-0088, CVE-2015-0090, CVE-2015-0091, CVE-2015-0092 a CVE-2015-0093 ovládača Adobe Font spôsobené nesprávnym prepísaním objektov v pamäti umožňujú útočníkovi vzdialené spustenie škodlivého kódu v kernel-móde s oprávneniami administrátora. Zraniteľnosti je možné zneužiť pri zobrazení infikovanej stránky alebo škodlivého súboru.

Zraniteľnosť CVE-2015-1637 umožňuje obídenie bezpečnosti v implementácii Microsoft Secure Channel (SChannel) prostredníctvom techniky TLS FREAK. Zraniteľnosť je možné zneužiť na útok typu Man-in-the-Middle, pri ktorom je vynútené použitie kratších kľúčov v šifrovaní TLS a následne je možné dešifrovať zabezpečenú komunikáciu.

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 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 MS15-019, MS15-020, MS15-021, MS15-031. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú pravdepodobne používané. Správcom systémov odporúčame prezrieť si marcové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-019
https://technet.microsoft.com/library/security/MS15-020
https://technet.microsoft.com/library/security/MS15-021
https://technet.microsoft.com/library/security/MS15-031

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2015-0085 spôsobená opätovným použitím uvoľnenej pamäte umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor.

Zraniteľnosť CVE-2015-0086 spôsobená poškodením pamäte počas práce s RTF dokumentmi umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor.

Zraniteľnosť CVE-2015-0097 spôsobená chybou pri práci s objektmi v pamäti počas spracovania dokumentov Office umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor.

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 (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
Microsoft Office 2013 RT Service Pack 1

Microsoft Word Viewer
Microsoft Excel 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 MS15-022. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú pravdepodobne používané.
Správcom systémov odporúčame prezrieť si marcový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:

https://technet.microsoft.com/library/security/MS15-022

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na zraniteľnosti, z ktorých 10 je označených ako kritických. Sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Na zraniteľnosť Internet Explorera s označením CVE-2015-0072 bol zaznamenaný exploit umožňujúci zvýšenie oprávnení prostredníctvom XSS útoku, čo uľahčuje zneužitie iných zraniteľností napríklad na vzdialené spustenie škodlivého kódu s oprávneniami užívateľa. Na mnohé ďalšie zraniteľnosti 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 MS15-018. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko už boli zaznamenané exploity na niektoré zraniteľnosti. Správcom systémov odporúčame prezrieť si marcový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/library/security/MS15-018

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci marec dve aktualizácie prehliadača Firefox opravujúce 15 zraniteľností, z toho 6 označených ako kritických.

Zraniteľnosť CVE-2015-0817 spôsobená chybou pri kontrole hraníc polí v JavaScriptovej Just-in-time kompilácii umožňuje vzdialené spustenie škodlivého kódu.

Zraniteľnosť CVE-2015-0818 spôsobená chybou pri práci s obrázkami SVG umožňuje zvýšenie oprávnení a v kombinácii s inou zraniteľnosťou môže byť zneužitá na spustenie škodlivého kódu so zvýšenými oprávneniami.

Zraniteľnosť CVE-2015-0813 spôsobená chybou pri prehrávaní MP3 súborov pomocou Fluendo MP3 pluginu pre GStreamer na Linuxe umožňuje vzdialené spustenie škodlivého kódu alebo spôsobiť pád aplikácie pri prehrávaní škodlivého MP3 súboru.

Zraniteľnosti CVE-2015-0805 a CVE-2015-0806 spôsobené chybami pri práci s pamäťou (nesprávne volania memset) počas renderovania 2D grafiky umožňujú vzdialené spustenie škodlivého kódu alebo spôsobiť pád aplikácie.

Zraniteľnosti CVE-2015-0803 a CVE-2015-0804 spôsobené opätovným použitím uvoľnenej pamäte pri práci elementmi Source umožňujú vzdialené spustenie škodlivého kódu alebo spôsobiť pád aplikácie.

Zraniteľnosť CVE-2015-0799 umožňuje potlačiť zobrazenie varovania o nesprávnom SSL certifikáte pri použití http/2 protokolu a Alt-Svc hlavičky, čo môže viesť k Man-in-the-Middle útoku, podstrčeniu falošného certifikátu a prístupu k zabezpečenej komunikácii.

Zraniteľné systémy:
Mozilla Firefox 36 a predchádzajúce
Mozilla Firefox ESR 31.5 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 37.0.1 a Mozilla Firefox ESR 31.6)
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 piatich bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť CVE-2015-1233 spôsobená chybou v interakcii medziprocesovej komunikácie, JavaScriptového enginu V8 a Gamepad API umožňuje vzdialenému útočníkovi spustiť škodlivý kód.

Zraniteľné systémy:
Google Chrome do verzie 41.0.2272.118

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

Zdroje:
http://googlechromereleases.blogspot.in/2015/03/stable-channel-update.html
http://googlechromereleases.blogspot.in/2015/03/stable-channel-update_10.html
http://googlechromereleases.blogspot.in/2015/03/stable-channel-update_19.html
http://googlechromereleases.blogspot.in/2015/04/stable-channel-update.html

4. Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci marec aktualizáciu opravujúcu 11 zraniteľností. Väčšina zraniteľnosti je spôsobená rôznymi chybami pri práci s pamäťou. Zraniteľnosti umožňujú vzdialenému útočníkovi spustenie škodlivého kódu.

Zraniteľné systémy:

Adobe Flash Player verzie 16.0.0.305 a nižšej
Adobe Flash Player verzie 13.0.0.269 a nižšej
Adobe Flash Player verzie 11.2.202.442 a nižšej

Odporúčania:

Užívateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 17.0.0.134, užívateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 13.0.0.277. Užívateľom Linux odporúčame aktualizovať na verziu 11.2.202.451. 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:

https://helpx.adobe.com/security/products/flash-player/apsb15-05.html

5. Frameworky

Microsoft .NET Framework

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

Zdroje:

https://technet.microsoft.com/library/security/ms15-mar

Oracle Java

Spoločnosť Oracle v mesiaci marec žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 14. apríl 2015.

Zdroje:

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

6. Iné závažné zraniteľnosti

FREAK útok

FREAK je útok na zraniteľnosť v implementáciách SSL/TLS protokolov umožňujúci vynútiť použitie kratších kľúčov pri Man-in-the-Middle útoku.

Šifrovanie s použitím kratších kľúčov je možné z dôvodu podpory tzv. exportných šifrovacích súprav, ktoré predstavujú zámerne oslabené verzie šifier určených na export mimo USA. Tieto verzie oslabených algoritmov sú prítomné v mnohých implementáciách SSL/TLS, a niektoré implementácie umožňujú vynútiť ich použitie namiesto plnohodnotných neoslabených algoritmov. Útočník tak môže vypočítať kratšie kľúče a následne zašifrovanú komunikáciu dešifrovať.

Zdroje:

https://www.smacktls.com/