Mesačný prehľad kritických zraniteľností
Február 2015

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2015-0008 systémov zapojených do domény pri získavaní a aplikovaní Skupinovej politiky umožňuje vzdialené spustenie škodlivého kódu a prevzatie kontroly nad zariadením. Na úspešné zneužitie zraniteľnosti je potrebné, aby sa počítač s nakonfigurovaným systémom s podporou domény pripojil do siete kontrolovanej útočníkom.

Zraniteľnosť CVE-2015-0059 vo Windows kernel-mode driver (Win32k.sys) spôsobená nesprávnym spracovaním TrueType fontov. Otvorenie dokumentu alebo webovej stránky so škodlivými TrueType fontami môže útočníkovi umožniť 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 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 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 MS15-010 a MS15-011. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si februárové Microsoft Security Bulletiny dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-010
https://technet.microsoft.com/library/security/MS15-011

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2015-0063, CVE-2014-0064 a CVE-2015-0065 spôsobené chybami pri práci s objektmi v pamäti pri spracovaní nekorektných dokumentov. Zraniteľnosti umožňujú vzdialené spustenie škodlivého kódu po otvorení infikovaného dokumentu Microsoft Office.

Zraniteľné systémy:
Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-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 Office Web Apps 2010 Service Pack 2

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-012. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú pravdepodobne používané.
Správcom systémov odporúčame prezrieť si februárový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-012

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na zraniteľnosti, z ktorých najzávažnejšie umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.
Na zraniteľnosť Internet Explorera s označením CVE-2015-0071 bol zaznamenaný exploit umožňujúci obísť zabezpečenie ASLR, čo uľahčuje zneužitie iných zraniteľností napríklad na vzdialené spustenie škodlivého kódu. 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 MS15-009. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko už boli zaznamenané exploity na niektoré zraniteľnosti. Správcom systémov odporúčame prezrieť si februárový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/library/security/MS15-009

Mozilla Firefox

Spoločnosť Mozilla vydala aktualizáciu pluginu OpenH264 a tiež novú verziu prehliadača Firefox opravujúcu 16 zraniteľností, z toho sú tri označené ako kritické.
Zraniteľnosť CVE-2015-0829 spôsobená chybou typu buffer overflow v knižnici libstagefright počas prehrávania MP4 súborov umožňuje vzdialené spustenie škodlivého kódu.
Zraniteľnosť CVE-2015-0831 spôsobená opätovným použitím už uvoľnenej pamäte pri vytváraní indexu v IndexedDB umožňuje vzdialené spustenie škodlivého kódu alebo spôsobenie pádu aplikácie pri spracovávaní infikovaného obsahu.
Viaceré bližšie nešpecifikované zraniteľnosti pri práci s pamäťou (CVE-2015-0835, CVE-2015-0836) môžu byť zneužité útočníkom na spôsobenie pádu aplikácie a možné spustenie škodlivého kódu.
Zraniteľnosť pluginu OpenH264 spôsobená nesprávnym spracovaním vstupu od užívateľa umožňuje spôsobiť pád aplikácie alebo možné spustenie škodlivého kódu po zobrazení infikovaného obsahu.

Zraniteľné systémy:
Mozilla Firefox 35 a predchádzajúce
Mozilla Firefox ESR 31.4 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 36.0 a Mozilla Firefox ESR 31.5)
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/
http://tools.cisco.com/security/center/viewAlert.x?alertId=37376

Google Chrome

Spoločnosť Google vydala dve aktualizácie prehliadača Chrome, ktoré obsahujú opravy 11 bezpečnostných opráv.
Najzávažnejšie zraniteľnosti umožňujú vzdialeným útočníkom vykonať útoky typu zamietnutie služby (spôsobiť pád aplikácie), eskaláciu privilégií, obídenie politiky SameOrigin, prípadne môžu mať iný bližšie nešpecifikovaný dôsledok.

Zraniteľné systémy
Google Chrome do verzie 40.0.2214.111

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 40.0.2214.111, prípadne na novšiu verziu 40.0.2214.115. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2015/02/stable-channel-update.html
http://googlechromereleases.blogspot.in/2015/02/stable-channel-update_19.html

4. Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci február dve aktualizácie opravujúce 19 zraniteľností. Väčšina zraniteľnosti je spôsobená rôznymi chybami pri práci s pamäťou ako opätovné použitie uvoľnenej pamäte, dereferencovanie nulových ukazovateľov, buffer overflow. Zraniteľnosti umožňujú vzdialenému útočníkovi spustenie škodlivého kódu.
Opravená je aj zraniteľnosť CVE-2015-031, ktorá sú spôsobená opätovným použitím uvoľnenej pamäte. Začiatkom mesiaca na ňu bol objavený a používaný exploit ešte pred vydaním opravy.

Zraniteľné systémy
Adobe Flash Player verzie 16.0.0.296 a nižšej

Adobe Flash Player verzie 13.0.0.264 a nižšej
Adobe Flash Player verzie 11.2.202.440 a nižšej

Odporúčania:
Užívateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 16.0.0.305, užívateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 13.0.0.269. Užívateľom Linux odporúčame aktualizovať na verziu 11.2.202.442. 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/apsb15-04.html
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=128

5. Frameworky

Microsoft .NET Framework

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

Zdroje:
https://technet.microsoft.com/library/security/ms15-feb

Oracle Java

Spoločnosť Oracle nevydala v mesiaci žiadnu aktualizáciu 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

Malware Superfish

Na notebookoch spoločnosti Lenovo bol v období od septembra 2014 do februára 2015 predinštalovávaný nástroj SuperFish, ktorý podľa oficiálneho vyjadrenia spoločnosti Lenovo mal pomáhať zobrazovať cielené reklamy. Softvér SuperFish však nainštaloval do systému podvrhnutý certifikát koreňovej autority, na základe ktorého generoval certifikáty pre navštívené stránky a zachytával tak nielen http, ale aj https komunikáciu užívateľa, čím sa správal ako malware.

Po odhalení a publikovaní informácii o softvéri SuperFish spoločnosť Lenovo tento nástroj prestala inštalovať do svojich zariadení a na svojich stránkach zverejnila návod na jeho odstránenie dostupný na odkaze:
http://support.lenovo.com/us/en/product_security/superfish_uninstall

Zraniteľné zariadenia:

E10-30
Flex2 14, Flex2 15, Flex2 14D, Flex2 15D, Flex2 Pro, Flex 10
G410, G510, G710, G40-30, G40-45, G40-70, G40-80, G50-50, G50-45, G50-70, G50-80, G50-80Touch
Miix2 – 8, Miix2 – 10, Miix2 – 11, Miix 3 - 1030
S310, S410, S415, S415 Touch, S435, S20-30, S20-30 Touch, S40-70
U330P, U430P, U330 Touch, U430 Touch, U530 Touch
Y430P, Y40-70, Y40-80, Y50-70, Y70-70
Yoga2-11, Yoga2-13, Yoga2Pro-13, Yoga3 Pro
Z40-70, Z40-75, Z50-70, Z50-75, Z70-80

Zdroje:

http://support.lenovo.com/en/product_security/superfish