Mesačný prehľad kritických zraniteľností
Február 2018

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2018-0825 v StructuredQuery je spôsobená nesprávnou prácou s objektmi v pamäti. Útočník, ktorý využije túto chybu môže spustiť ľubovoľný kód ako práve prihlásený používateľ. Ak je používateľ admin, potom útočník môže prebrať kontrolu nad systémom. Hrozí teda spustenie programov s administrátorskými právami a to, že útočník prevezme kontrolu nad zariadením. Útočník, ktorý získal práva admina môže meniť a mazať údaje a taktiež vytvárať nové účty s administrátorskými právami. Na zneužitie tejto zraniteľnosti je potrebné aby používateľ otvoril špeciálne vytvorený súbor, ktorý používateľ môže dostať e-mailom.

Zraniteľné systémy:

Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1511 for 32-bit Systems
Windows 10 Version 1511 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems
Windows 10 Version 1709 for 32-bit Systems
Windows 10 Version 1709 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
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 Itanium-Based Systems Service Pack 2
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 R2 for Itanium-based Systems Service Pack 1
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 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server, version 1709 (Server Core installation)

Odporúčania:

Vzhľadom na závažnosť uvedenej zraniteľnosti odporúčame bezodkladne aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0825

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2018-0852 produktu Outlook je spôsobená chybou pri práci s objektmi v pamäti. Umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami používateľa, ktorý otvorí infikovaný súbor. Ak je používateľ administrátor, útočník môže prevziať kontrolu nad systémom používateľa. Táto zraniteľnosť je nebezpečná aj preto, že samotný Preview Pane Outlooku je útočným vektorom takže aj zobrazenie e-mailu v paneli umožní spustenie takéhoto kódu.

Zraniteľné systémy:

Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions
Microsoft Outlook 2007 Service Pack 3
Microsoft Outlook 2010 Service Pack 2 (32-bit editions)
Microsoft Outlook 2010 Service Pack 2 (64-bit editions)
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)

Odporúčania:

Vzhľadom na závažnosť uvedenej zraniteľnosti odporúčame bezodkladne aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0852
https://threatpost.com/two-nasty-outlook-bugs-fixed-in-microsofts-feb-patch-tuesday-update/129931/

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci januárového balíka opráv boli spoločnosťou Microsoft vydané opravy jednej kritickej zraniteľnosti.
Zraniteľnosť CVE-2018-0840 umožňuje útočníkovi vzdialene vykonať kód. Je spôsobená tým, ako skriptovací engine narába s objektmi v pamäti. Útočník vie zneužiť túto zraniteľnosť, ak presvedčí používateľa aby navštívil jeho špeciálne vytvorenú webstránku. Útočník taktiež môže do aplikácie alebo MS Office dokumentu vložiť ovládací prvok ActiveX označený ako bezpečný na inicializáciu. Úspešné zneužitie dáva útočníkovi možnosť získať právomoci aktuálneho používateľa. Ak má prihlásený užívateľ administrátorské právomoci, útočník môže prevziať kontrolu nad systémom, inštalovať programy, prezerať, meniť a mazať dáta, či vytvárať nové užívateľské účty s administrátorskými právami.

Zraniteľné systémy:

ChakraCore

Microsoft Internet Explorer 10-11

Odporúčania:

Vzhľadom na závažnosť uvedenej zraniteľnosti odporúčame bezodkladne aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania. Nakoľko na túto zraniteľnosť existuje verejne dostupný exploit odporúčame aktualizácie vykonať čo najskôr.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0840

Microsoft Edge

Zraniteľnosť CVE-2016-0840 sa týka aj prehliadača Internet explorer pre bližší popis viď časť Microsoft Internet Explorer.
Zraniteľnosti CVE-2018-0859 až CVE-2018-0861 spočívajú v spôsobe, akým skriptovací engine narába s objektmi v pamäti. Ich zneužitím možno zapríčiniť narušenie integrity pamäte spôsobom, ktorý umožní útočníkovi spúšťať ľubovoľný kód s takými právami ako má aktuálny používateľ. Útočník musí presvedčiť používateľa, aby navštívil jeho špeciálne vytvorenú webstránku, navrhnutú na zneužitie zraniteľnosti cez internetový prehliadač Edge. Útočník môže umiestniť špeciálny obsah určený na zneužitie zraniteľnosti aj na kompromitovanú webstránku, alebo webstránku s užívateľským obsahom či reklamou. Ak má prihlásený užívateľ administrátorské právomoci, útočník môže prevziať kontrolu nad systémom, inštalovať programy, prezerať, meniť a mazať dáta, či vytvárať nové užívateľské účty s používateľskými právami.
Zraniteľnosť CVE-2018-0858 je spôsobená tým, že skriptovací engine ChakraCore nesprávne spracováva objekty v pamäti. Pamäť môže byť teda poškodená takým spôsobom, že útočník môže spustiť ľubovoľný kód ako daný používateľ. Útočník s administrátorskými právami môže zobrazovať, meniť a mazať údaje, inštalovať programy.
Kritická zraniteľnosť CVE-2018-0763 umožňuje útočníkovi spôsobiť únik informácií, zneužitím chyby pri narábaní s objektmi v pamäti. Útočník môže túto zraniteľnosť zneužiť tak, že

presvedčí používateľa, aby navštívil jeho špeciálne vytvorenú webstránku. Útočník môže umiestniť špeciálny obsah určený na zneužitie zraniteľnosti aj na kompromitovanú webstránku, alebo webstránku s užívateľským obsahom či reklamou. Získané informácie môže útočník zneužiť na ďalšiu kompromitáciu používateľovho systému

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzií 1511, 1607, 1703 a 1709 a 32-bitových aj 64-bitových verziách
Microsoft Edge v systéme Windows Server 2016

Odporúčania:

Vzhľadom na závažnosť uvedenej zraniteľnosti odporúčame bezodkladne aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania. Nakoľko na niektoré z týchto existujú verejne dostupné exploity odporúčame aktualizácie vykonať čo najskôr

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0763
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0840
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0856
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0857
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0859
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0858
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0860
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0861

Mozilla Firefox

Spoločnosť Mozilla nevydala v mesiaci február pre aplikáciu Mozilla Firefox žiadne opravy kritických zraniteľností.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/

Google Chrome

Spoločnosť Google vydala aktualizácie prehliadača Chrome, ktoré obsahujú opravy 1 kritickej bezpečnostnej zraniteľnosti. Konkrétne sa jedná o zraniteľnosť CVE-2018-6056 nesprávnej inštancie odvodenej triedy.

Odporúčania:

Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na verziu 64.0.3282.167/168, prípadne novšiu. V prípade potreby odporúčame aplikovať aktualizáciu ručne cez menu otvorením okna s aktuálne nainštalovanou verziou, čo zároveň spustí aj kontrolu dostupnosti aktualizácie.

Zdroje:
https://chromereleases.googleblog.com/2018/02/stable-channel-update-for-desktop_13.html
https://chromereleases.googleblog.com/2018/02/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci február aktualizácie opravujúce 41 zraniteľností. Najzávažnejšou z nich je CVE-2018-4878. Táto zraniteľnosť môže viesť k spusteniu kódu v Adobe Flash Player 28.0.0.137 a starších. Je zaznamenaný exploit pre CVE-2018-4878, ktorý bol využitý v cielených útokoch na používateľov OS Windows. Útoky využívajú dokumenty balíka Office s vloženým škodlivým kódom Flash distribuovaným pomocou emailu.

Zraniteľné systémy:
Acrobat DC (Continuous Track) 2018.009.20050 a staršie
Acrobat Reader DC (Continuous Track) 2018.009.20050 a staršie
Acrobat 2017 2017.011.30070 a staršie
Acrobat Reder2017 2017.011.30070 a staršie
Adobe Flash Player verzie 28.0.0.137 a staršie
Acrobat DC (Classic Track) 2015.006.30394 a staršie
Acrobat Reader DC (Classic Track) 2015.006.30395 a staršie

Odporúčania:
Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy. Jedná sa najmä o Adobe Flash Player, ktorý treba aktualizovať na verziu 28.0.0.161, nakoľko bolo zaznamenané použitie exploitov na zraniteľnosť tohto systému.
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/apsa18-01.html
https://helpx.adobe.com/security/products/flash-player/apsb18-03.html
https://helpx.adobe.com/security/products/acrobat/apsb18-02.html
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180004
https://threatpost.com/remote-code-execution-bug-patched-in-adobe-acrobat-reader-dc/130109/

5. Frameworky

Microsoft .NET Framework

Pre Microsoft .NET Framework neboli vo februári žiadne aktualizácie.

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

Oracle Java

Spoločnosť Oracle v mesiaci február žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 17. apríl 2018.

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

6. Iné závažné zraniteľnosti

Lenovo

Spoločnosť Lenovo zaznamenala, že dve kritické zraniteľnosti spoločnosti Broadcom ovplyvňujú 25 modelov značky ThinkPad. Zraniteľnosti boli odhalené už v septembri, ale pôvodne bolo známe len to, že postihli špecifické čipové súpravy Broadcom používané v telefónoch Apple iPhone, Apple TV a Android.
Podľa spoločnosti Lenovo zraniteľnosti CVE-2017-11120 a CVE-2017-11121 zasiahli aj chipsety Wi-Fi, ktoré sa nachádzajú v ThinkPadoch. Takto rozšírila zoznam zasiahnutých zariadení o dve desiatky ThinkPadov, ktoré používajú ovládač Broadcom pre bezdrôtovú sieť LAN.
Ovládač siete Broadcom Wireless LAN obsahuje chybu pretečenia vyrovnávacej pamäte, čo môže spôsobiť, že útočník môže spustiť ľubovoľný kód na adaptéri, nie však na CPU cieľového systému. Pri úspešnom exploite je možné jednoduché diaľkové ovládanie čipu Wi-Fi.
Zraniteľnosť CVE-2017-11121 je taktiež chybou pretečenia vyrovnávacej pamäte. Je spôsobená nesprávnou validáciou signálov Wi-Fi. Pri správnom vytvorení bezdrôtových rámcov rýchleho prechodu je možné pretečenie zásobníkov, čo môže viesť ku odmietaniu služieb.
Tieto zraniteľnosti ovplyvnili platformy iOS, tvOS spoločnosti Apple a Android spoločnosti Google. Pre tieto zraniteľnosti boli vydané záplaty už v septembri.

Spoločnosť Lenovo taktiež zaznamenala zraniteľnosť vo svojom softvéri Fingerprint Manager Pro, ktorý by mohol umožniť únik citlivých údajov uložených používateľmi. Softvér umožňuje používateľom pristupovať k počítačom Lenovo pomocou odtlačku prsta a môže byť taktiež nakonfigurovaný na ukladanie poverení webových stránok a autentifikáciu stránok pomocou odtlačku prsta. Softvér teda ukladá citlivé informácie ako prihlasovacie údaje do systému Windows a sú šifrované pomocou slabého kryptografického algoritmu.
Zraniteľnosť CVE-2017-3762 spočívajúca v zadrôtovanom hesle robí údaje uložené softvérom prístupné pre všetkých užívateľov aj bez administrátorského prístupu.

Zraniteľné systémy:
Zraniteľnosti CVE-2017-11120 a CVE-2017-11121 sa týkajú: ThinkPad 10, ThinkPad L460, ThinkPad P50s, ThinkPad T460, ThinkPad T460p, ThinkPad T460s, ThinkPad T560, ThinkPad X260, ThinkPad Yoga 260.
Zariadenia kompatibilné s Fingerprint Manager Pro:
ThinkPad L560
ThinkPad P40 Yoga, P50
ThinkPad T440, T440, T440, T450, T450, T450, T540, T550, T560
ThinkPad W540, W541, W550

ThinkPad X1 Carbon (typ 20A7, 20A8), X1 Carbon (typ 20BS, 20BT)
ThinkPad X240, X240, X250, X260
ThinkPad Yoga 14 (20FY), Yoga 460
ThinkCentre M73, M73z, M78, M79, M83, M93, M93p, M93z
ThinkStation E32, P300, P500, P700, P900

Odporúčania:

Odporúčame aktualizovať verzie ovládačov Wi-Fi a taktiež aktualizovať Fingerprint Manager Pro na verziu 8.01.87 alebo novšiu. Link na stránku Lenova kde je možné nájsť aktualizácie nájdete nižšie.

Zdroje:

https://pcsupport.lenovo.com/sk/en/downloads/ds034486
https://threatpost.com/lenovo-warns-critical-wifi-vulnerability-impacts-dozens-of-thinkpad-models/129860/
https://thehackernews.com/2018/01/lenovo-fingerprint.html

Cisco

Vo firewall softvéri Adaptive Security Appliance spoločnosti Cisco sa objavila kritická zraniteľnosť. Úspešný útočník by mohol zobraziť všetky údaje v systéme, získať administrátorské oprávnenia a vzdialený prístup k sieti. Využitie zraniteľnosti by taktiež mohlo spôsobiť zlyhanie brány firewall a mohlo by narušiť pripojenie k sieti. Bol zverejnený ukážkový exploit spôsobujúci pád systému.
Spoločnosť Cisco vydala záplatu na túto zraniteľnosť, avšak po pár dňoch ju aktualizovala, pretože sa našli ďalšie útočné vektory a funkcie. Zraniteľnosť je spojená s ASA XML parserom. Škodlivý XML súbor môže umožniť vykonať ľubovoľný kód a získať plnú kontrolu nad systémom. Taktiež môže spôsobiť opätovné načítanie zariadenia a zastavenia spracovania prichádzajúcich žiadostí o autentifikáciu VPN.

Zraniteľné systémy:

prístroj na ochranu priemyselných bezpečnostných sád 3000
adaptéry ASA 5500 Adaptive Security Series ASA 5500-X série
virtuálne zariadenie Adaptive Security
zariadenia Firepower Security
softvér Firewall Threat Defense Software.

Zdroje:

https://threatpost.com/cisco-confirms-critical-firewall-software-bug-is-under-attack/129858/

Exim

Zraniteľnosť CVE-2018-6789 poštového serveru Exim je zraniteľnosťou pretečenia zásobníka. Off-by-one chyba môže útočníkovi umožniť vzdialené spustenie ľubovoľného kódu. Zraniteľnými sa stalo veľké množstvo serverov keďže sa chyba v Exime nachádza už od začiatku. Záplata na túto zraniteľnosť už bola vydaná a zraniteľnými sú všetky verzie Eximu staršie ako 4.90.1. Odporúčame teda čo najskôr aktualizovať na verziu 4.90.1.

Zdroje:
https://www.root.cz/zpravicky/chyba-v-mail-serveru-exim-umoznuje-vzdalene-spusteni-kodu/