Mesačný prehľad kritických zraniteľností
Január 2019

1. Operačné systémy Microsoft Windows

V mesiaci január vydala spoločnosť Microsoft opravy na tri kritické zraniteľnosti týkajúce sa operačného systému Windows.
Všetky tri zraniteľnosti umožňujú vzdialené vykonávanie kódu. Zraniteľnosť CVE-2019-0547 sa nachádza vo Windows DHCP klientovi a súvisí s poškodením pamäte pri narábaní s istými DHCP odpoveďami. Útočník tak môže zraniteľnosť zneužiť odoslaním špeciálne vytvorenej DHCP odpovede. Ďalšie dve opravené kritické zraniteľnosti CVE-2019-0550 a CVE-2019-0551 súvisia so situáciou, keď Windows Hyper-V na hostiteľskom serveri nesprávne vyhodnotí vstup od prihláseného používateľa na hosťovskom systéme. Ak útočník spustí na hosťovskom systéme vhodne vytvorenú aplikáciu, umožní mu to vykonávať ľubovoľný kód na hostiteľskom systéme.
Zároveň bola tento mesiac objavená jedna zero-day zraniteľnosť v aplikácii Windows Contacts, ktorá umožňuje vzdialené vykonávanie kódu. Opravu vydala spoločnosť 0patch, spoločnosť Microsoft zatiaľ opravu neplánuje. Viac sa o tejto zraniteľnosti môžete dočítať tu.

Zraniteľné systémy:

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 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server, version 1709 (Server Core installation)
Windows Server, version 1803 (Server Core installation)

Odporúčania:

Vzhľadom na závažnosť kritických zraniteľností 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-2019-0547
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0550
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0551

2. Kancelárske balíky Microsoft Office a Office Web Apps

V balíkoch Microsoft Office bolo tento mesiac opravených jedenásť závažných zraniteľností.
Zraniteľnosť CVE-2019-0562 umožňuje zvýšenie práv a nastáva keď Microsoft SharePoint Server nesprávne sanitizuje špeciálne vytvorenú webovú požiadavku. Zneužitie tejto zraniteľnosti umožní útočníkovi vykonávať útoky typu cross-site-scripting a vykonávanie skriptov s právami práve prihláseného používateľa. Tieto útoky môžu ďalej spôsobiť, že útočník môže vidieť obsah na SharePoint stránke, ku ktorému nemá právo pristupovať, a tiež vykonávať akcie ako zmazanie či vloženie škodlivého obsahu.
Tri zraniteľnosti umožňujú vzdialené vykonávanie kódu. CVE-2019-0541 súvisí s nesprávnym vyhodnocovaním vstupu nástrojom MSHTML. Na zneužitie môže útočník presvedčiť obeť, aby sa pokúsila upraviť špeciálne vytvorený HTML súbor. CVE-2019-0585 sa nachádza v aplikácii Microsoft Word, ktorá nesprávne narába s objektmi v pamäti. Pre zneužitie je možné použiť špeciálne pripravený súbor, ktorý obeť otvorí v zraniteľnej verzii MS Word. Útočník môže taktiež využiť špeciálne vytvorenú stránku, pričom odkaz na ňu pošle používateľovi. Po úspešnom zneužití jednej z týchto zraniteľností, môže útočník získať právo vykonávať škodlivý kód ako práve prihlásený používateľ. V prípade, že bol používateľ prihlásený ako administrátor získa útočník možnosť inštalovať programy; zobrazovať, meniť alebo mazať dáta; či vytvárať plnohodnotné účty. Zraniteľnosť CVE-2019-0582 je spôsobená nesprávnym narábaním s objektmi v pamäti aplikáciou Windows Jet Database Engine. Útočník môže opäť využiť špeciálne pripravený súbor a po úspešnom zneužití získa možnosť vykonávať ľubovoľný kód.
Zraniteľnosti CVE-2019-0559, CVE-2019-0560 a CVE-2019-0561 spôsobujú únik informácií. Prvá sa týka aplikácie Microsoft Outlook, ktorá nesprávne narába s istými typmi správ a odhaľuje informácie o obeti. Útočník môže zraniteľnosť využiť zaslaním špeciálne vytvoreného e-mailu. Druhá zraniteľnosť súvisí s nesprávnym zverejňovaním informácií v pamäti balíkom Microsoft Office a útočníkovi dáva informácie o počítači a dáta obete. Útočník môže presvedčiť obeť, aby otvorila špeciálne pripravený súbor, no musí tiež poznať adresu v pamäti, kde bol objekt vytvorený. Tretia zraniteľnosť súvisí s nesprávnym použitím gombíkov makier v Microsoft Word. Útočníkovi umožňuje čítať ľubovoľné súbory v systéme obete. Útočník môže presvedčiť obeť, aby otvorila špeciálne pripravený súbor, no musí tiež poznať lokáciu súboru, ktorý chce čítať.
Posledné štyri zraniteľnosti CVE-2019-0556, CVE-2019-0557, CVE-2019-0558, CVE-2019-0624 umožňujú predstierať cudziu identitu (spoofing). Prvé tri súvisia s aplikáciou SharePoint Server, ktorá nevhodne sanitizuje špeciálne vytvorenú webovú požiadavku. Zneužitie tejto zraniteľnosti umožní útočníkovi vykonávať útoky typu cross-site-scripting a vykonávanie skriptov s právami práve prihláseného používateľa. Tieto útoky môžu ďalej spôsobiť, že

útočník môže vidieť obsah na SharePoint stránke, ku ktorému nemá právo pristupovať, a tiež vykonávať akcie ako zmazanie či vloženie škodlivého obsahu. Štvrtá zraniteľnosť existuje v nevhodnej sanitizácii špeciálne vytvorených požiadavku pre server Skype for Business 2015. Útočník môže obeti poslať špeciálne upravenú URL adresu, ktorá obeť privedie na cielenú stránku Skype for Business. To umožní útočníkovi vykonávať útoky typu cross-site-scripting a vykonávanie skriptov s právami práve prihláseného používateľa.

Zraniteľné systémy:

Microsoft Business Productivity Servers 2010 Service Pack 2
Microsoft Excel Viewer 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 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2016 for Mac
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office Online Server
Microsoft Office Web Apps Server 2010 Service Pack 2
Microsoft Office Word Viewer
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)
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft Word 2010 Service Pack 2 (32-bit editions)
Microsoft Word 2010 Service Pack 2 (64-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Office 365 ProPlus for 32-bit Systems

Office 365 ProPlus for 64-bit Systems
Skype for Business Server 2015 CU 8
Word Automation Services

Odporúčania:

Vzhľadom množstvo závažných zraniteľností 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-2019-0541
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0556
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0557
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0558
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0559
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0560
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0561
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0562
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0582
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0585
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0624

3. Internetové prehliadače

Microsoft Internet Explorer

V prehliadači Internet Explorer bola tento mesiac opravená jedna závažná zraniteľnosť. Umožňuje vzdialene vykonávať kód. CVE-2019-0541 súvisí s nesprávnym vyhodnocovaním vstupu nástrojom MSHTML. Na zneužitie môže útočník presvedčiť obeť, aby sa pokúsila upraviť špeciálne vytvorený HTML súbor. Po úspešnom zneužití zraniteľnosti, môže útočník získať právo spúšťať škodlivý kód ako práve prihlásený používateľ. V prípade, že bol používateľ prihlásený ako administrátor získa útočník možnosť inštalovať programy; zobrazovať, meniť alebo mazať dáta; či vytvárať plnohodnotné účty.

Zraniteľné systémy:

Microsoft Internet Explorer verzie 11

Odporúčania:

Vzhľadom na závažnosť kritickej 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-2019-0541

Microsoft Edge

V mesiaci január boli opravené štyri kritické zraniteľnosti v prehliadači Microsoft Edge, ktoré umožňujú vzdialene vykonávať kód. Tieto zraniteľnosti nesú označenie CVE-2019-0539, CVE-2019-0567, CVE-2019-0568 a CVE-2019-0565. Prvé tri sa nachádzajú v spôsobe, akým skriptovací nástroj Chakra narába s objektmi v pamäti. Pritom môže dôjsť k poškodeniu pamäte, čo umožní útočníkovi vykonávať kód s právami práve prihláseného užívateľa. V prípade, že bol používateľ prihlásený ako administrátor, získa útočník možnosť inštalovať programy; zobrazovať, meniť alebo mazať dáta; či vytvárať plnohodnotné účty. Pre útok je možné zneužiť špeciálne vytvorenú, alebo kompromitovanú webstránku, či stránku s používateľským obsahom a reklamou. Štvrtá zraniteľnosť súvisí so spôsobom, akým Microsoft Edge pristupuje k objektom v pamäti. Následky a spôsob zneužitia sú zhodné s predchádzajúcimi zraniteľnosťami.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzií 1607, 1703, 1709, 1803 a 1809, v 32-bitových, 64-bitových verziách aj ARM64 verzii
Microsoft Edge v systémoch Windows 10 32-bitových aj 64-bitových verziách

Odporúčania:

Vzhľadom na množstvo kritických zraniteľností 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-2019-0539
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0565
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0567
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0568

Mozilla Firefox

Spoločnosť Mozilla tento mesiac vo svojom prehliadači opravila tri kritické a tri závažné zraniteľnosti. Kritické zraniteľnosti sú označené CVE-2018-18500, CVE-2018-18501 a CVE-2018-18502. Prvá umožňuje použitie odalokovaného miesta v pamäti, čo môže nastať pri analýze HTML5 prúdu v súhre s istými HTML prvkami, pričom ďalšie dve sa týkajú poškodenia pamäte, ktoré by mohlo vyústiť až k tomu, že by útočník mohol vzdialene vykonávať kód.

Zraniteľné systémy:

Mozilla Firefox 64.0.2
Mozilla Firefox ESR 60.4

Zdroje:

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

https://www.mozilla.org/en-US/security/advisories/mfsa2019-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-02/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-03/

Google Chrome

Spoločnosť Google vydala tento mesiac aktualizácie, ktoré opravujú jednu kritickú zraniteľnosť a až sedemnásť závažných zraniteľností.

Zraniteľné systémy:

Google Chrome verzie staršie ako 72.0.3626.81

Zdroje:

https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/01/stable-channel-update-for-chrome-os.html
https://chromereleases.googleblog.com/2019/01/stable-channel-update-for-desktop.html

4. Adobe Flash Player, Acrobat a Reader

Tento mesiac spoločnosť Adobe vydala aktualizáciu produktu Adobe Flash Player, no neboli v nej opravené žiadne zraniteľnosti.
V produktoch Acrobat a Reader boli opravené dve kritické zraniteľnosti. CVE-2018-16011 dovoľuje vzdialene vykonávať kód, CVE-2018-16018 umožňuje zvýšenie práv.

Zraniteľné systémy:

Acrobat DC 2019.010.20064 a staršie
Acrobat Reader DC 2019.010.20064 a staršie
Acrobat 2017 2017.011.30110 a staršie
Acrobat Reader 2017.011.30110 a staršie
Acrobat DC 2015 2015.006.30461 a staršie
Acrobat Reader DC 2015 2015 2015.006.30461 a staršie

Odporúčania:

Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy nasledovne:

- Acrobat DC 2019.010.20069
- Acrobat Reader DC 2019.010.20069
- Acrobat 2017 2017.011.30113
- Acrobat Reader 2017 2017.011.30113
- Acrobat DC 2015 2015.006.30464
- Acrobat Reader DC 2015 2015.006.30464

Aktualizácie sú dostupné prostredníctvom stránky Adobe Acrobat Reader Download Center, Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Acrobat Reader.

Zdroje:

https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb19-02.html

https://helpx.adobe.com/security/products/flash-player/apsb19-01.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft tento mesiac nevydala pre Microsoft .NET Framework žiadne bezpečnostné aktualizácie.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

Oracle Java

Spoločnosť Oracle vydala v mesiaci január plánovanú štvrťročnú veľkú sadu aktualizácií. V produkte Java SE a Java SE Embedded bolo opravených len 6 stredne a nízko závažných zraniteľností.

Zraniteľné systémy:
Java Advanced Management Console 2.12
Java SE 7u201, 8u192, 11.0.1
Java SE Embedded 8u191

Odporúčania:
Napriek nízkej závažnosti uvedených zraniteľností odporúčame aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, prostredníctvom Java Auto Update, alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:
https://www.oracle.com/technetwork/topics/security/alerts-086861.html
https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html#AppendixJAVA

6. Iné závažné zraniteľnosti

Zraniteľnosť v správcovi APT pre Linux

Bola opravená kritická chyba v Linuxovom správcovi balíčkov APT umožňujúca pri presmerovávaní na zrkadlo útočníkovi vložiť do HTTP komunikácie upravený balíček, či škodlivý kód, ktorý správca APT vyhodnotí ako legitímny. Takto útočník dostáva možnosť vzdialene vykonávať ľubovoľný kód s právami root. Pre viac informácií si prečítajte naše varovanie.

Zraniteľné systémy:
Správca balíčkov APT, ktorý využívajú distribúcie Linuxu odvodené od Debian a Ubuntu, od verzie 0.8.15

Odporúčania:
Aktualizácia správcu balíčkov APT aspoň na verziu:

- Debian: Stretch 1.4.9, Jessie 1.0.9.8.5
- Ubuntu: 1.2.29ubuntu0.1, 1.7.0ubuntu0.1, 1.0.1ubuntu2.19, 1.6.6ubuntu0.1

Pri aktualizácii sa odporúča zakázať presmerovanie, aby nedošlo k zneužitiu zraniteľnosti.

Zero-day zraniteľnosť vo Windows Contacts

Bola opravená zraniteľnosť v aplikácii Windows Contacts umožňujúca útočníkovi vytvoriť škodlivú vizitku vo formáte .VCF, alebo .Contact. Keď na ňu obeť klikne, útočník môže vykonávať ľubovoľný kód s právami práve prihláseného užívateľa. Spoločnosť Microsoft neplánuje zraniteľnosť odstrániť. Záplatu vydala spoločnosť 0patch. Pre viac informácií si prečítajte naše varovanie.

Zraniteľné systémy:

Windows Vista - Windows 10

Odporúčania:

Pre verzie operačného systému Windows 10 v. 1803 (64-bit) a Windows 7 (64-bit) existuje mikrozáplata z platformy 0patch. Pre iné verzie Windows je možné o mikrozáplatu požiadať.