Mesačný prehľad kritických zraniteľností
December 2018

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft tento mesiac opravila dve kritické zraniteľnosti týkajúce sa operačného systému Windows.
Prvá zraniteľnosť s označením CVE-2018-8926 umožňuje vzdialené vykonávanie kódu. Zraniteľnosť sa nachádza vo Windows Domain Name System (DNS), ktoré nesprávne spracúva požiadavky. Po zneužití tejto zraniteľnosti môže útočník spúšťať kód ako Local System používateľ. Druhou opravenou zraniteľnosťou je CVE-2018-8634, ktorá taktiež umožňuje vzdialené vykonávanie kódu. Táto nastáva kvôli tomu že Microsoft text-to-speech nesprávne narába s objektmi v pamäti. Po zneužití je možné prevziať kontrolu nad systémom a útočník tak má možnosť inštalovať programy; prezerať, meniť či mazať dáta; vytvárať nových používateľov s plnými právami.
Okrem týchto dvoch kritických zraniteľností spoločnosť opravila taktiež jednu z dvoch zero-day zraniteľností, z ktorých prvá umožňuje zvýšenie práv a druhá dovoľuje zvýšenie práv a čítanie ľubovoľných súborov na úrovni systémových práv. O týchto zraniteľnostiach si môžete prečítať viac v našom varovaní 1 a 2.

Zraniteľné systémy:

Windows 10 for 32-bit Systems
Windows 10 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 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
Winsows Server 2012 R2
Winsows Server 2012 R2 (Server Core installation)
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-2018-8626
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8634

2. Kancelárske balíky Microsoft Office a Office Web Apps

V balíkoch Microsoft Office bolo tento mesiac opravených deväť závažných zraniteľností.
Zraniteľnosť CVE-2018-8635 je zraniteľnosťou zvýšenia práv a nastáva keď Microsoft SharePoint Server nesprávne vyčistí špeciálne vytvorenú autentifikačnú požiadavku. Po zneužití útočník môže vykonávať škodlivý kód na serveri. Ďalšou zraniteľnosťou Microsoft SharePoint Servera je CVE-2018-86650 a umožňuje cross-site-scripting útoky a vykonávanie skriptov ako práve prihlásený používateľ. Tieto útoky môžu ďalej spôsobiť, že útočník môže vidieť obsah na SharePoint stránke, ku ktorému nemá právo a vykonávať akcie ako zmazanie či vloženie obsahu.
Zraniteľnosti vzdialeného vykonávania kódu CVE-2018-8587, CVE-2018-8597, CVE-2018-8628 a CVE-2018-8636 sú spôsobené tým, že Microsoft Excel, Microsoft PowerPoint alebo Microsoft Outlook nesprávne narábajú s objektmi v pamäti. Na zneužitie je možné použiť špeciálne pripravený súbor. Útočník musí ešte presvedčiť používateľa, aby ten súbor otvoril. To môže urobiť zaslaním e-mailu alebo rýchlej správy. Útočník môže taktiež využiť špeciálne vytvorenú stránku, pričom odkaz na ňu pošle používateľovi. Po úspešnom zneužití jednej z týchto zraniteľností, 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.
Zraniteľnosti CVE-2018-8580, CVE-2018-8627 a CVE-2018-8598 spôsobujú únik informácií. Prvá zo spomínaných sa týka Microsoft SharePoint Servera a umožňuje vykonávať cross-site search útoky. Nastáva keď je používateľ súčasne prihlásený na Microsoft SharePoint Server a navštívi škodlivú webstránku. Útočník tak môže cez funkcie prehliadačov vykonať vyhľadávacie dopyty ako prihlásený používateľ. Druhé dve sa týkajú programu Microsoft Excel, ktorý nesprávne zverejňuje obsah pamäte. Útočník po zneužití môže použiť získané informácie na ďalšie škodlivé úkony.

Zraniteľné systémy:

Microsoft Excel 2010 Service Pack 2 (32-bitová verzia)
Microsoft Excel 2010 Service Pack 2 (64-bitová verzia)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bitová verzia)
Microsoft Excel 2013 Service Pack 1 (64-bitová verzia)

Microsoft Excel 2016 (32-bitová verzia)
Microsoft Excel 2016 (64-bitová verzia)
Microsoft Excel Viewer 2007 Service Pack 3
Microsoft Outlook 2010 Service Pack 2 (32-bitová verzia)
Microsoft Outlook 2010 Service Pack 2 (64-bitová verzia)
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (32-bitová verzia)
Microsoft Outlook 2013 Service Pack 1 (64-bitová verzia)
Microsoft Outlook 2016 (32-bitová verzia)
Microsoft Outlook 2016 (64-bitová verzia)
Microsoft PowerPoint 2010 Service Pack 2 (32-bitová verzia)
Microsoft PowerPoint 2010 Service Pack 2 (64-bitová verzia)
Microsoft PowerPoint 2013 RT Service Pack 1
Microsoft PowerPoint 2013 Service Pack 1 (32-bitová verzia)
Microsoft PowerPoint 2013 Service Pack 1 (64-bitová verzia)
Microsoft PowerPoint 2016 (32-bitová verzia)
Microsoft PowerPoint 2016 (64-bitová verzia)
Microsoft PowerPoint Viewer
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Foundation 2013 Service Pack 1
Office 365 ProPlus pre 32-bitové systémy
Office 365 ProPlus pre 64-bitové systémy
Office Online Server
Microsoft Office 2010 Service Pack 2 (32-bitová verzia)
Microsoft Office 2010 Service Pack 2 (64-bitová verzia)
Microsoft Office 2016 pre Mac
Microsoft Office 2019 pre Mac
Microsoft Office 2019 (32-bitová verzia)
Microsoft Office 2019 (64-bitová verzia)
Microsoft Office Compatibility Pack Service Pack 3

Odporúčania:

Vzhľadom na 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-2018-8635
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8650

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8587
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8597
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8628
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8636
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8627
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8598
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8580

3. Internetové prehliadače

Microsoft Internet Explorer

V prehliadači Internet Explorer bola tento mesiac opravená iba jedna kritická zraniteľnosť. Ide o zraniteľnosť spôsobujúcu poškodenie pamäte, ktorú môžete nájsť pod označením CVE-2018-8631. Je spôsobená nesprávnym narábaním prehliadača Internet Explorer s objektmi v pamäti. Môže spôsobiť také poškodenie pamäte, že útočník získa možnosť spúšťať kód ako práve prihlásený používateľ. Ak je práve prihláseným používateľom administrátor, získa útočník právo inštalovať programy; prezerať, mazať alebo meniť dáta; či vytvárať ďalšie plnohodnotné účty. Na jej zneužitie musí útočník presvedčiť používateľa aby navštívil špeciálne vytvorenú stránku, ktorej odkaz môže poslať napríklad pomocou emailu alebo rýchlej správy.
Okrem tejto zraniteľnosti bola opravená aj jedna zero-day zraniteľnosť, ktorá umožňuje vykonávanie ľubovoľného kódu. Prečítajte si viac o tejto zraniteľnosti v našom varovaní.

Zraniteľné systémy:

Microsoft Internet Explorer verzie 9, 10, 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-2018-8631

Microsoft Edge

Päť kritických zraniteľností bolo opravených tento mesiac v prehliadači Microsoft Edge, pričom zneužitie týchto zraniteľností môže poškodiť pamäť. Opravenými zraniteľnosťami sú: CVE-2018-8583, CVE-2018-8617, CVE-2018-8618, CVE-2018-8624 a CVE-2018-8629. Postup zneužitia a možné dôsledky sú rovnaké ako pri zraniteľnostiach spomínaných pre Internet Explorer.

Zraniteľné systémy:

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

Microsoft Edge v systémoch Windows 10 32-bitových aj 64-bitových verziách
Microsoft Edge v systéme Windows Server 2016
Microsoft Edge v systéme Windows Server 2019

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-2018-8583
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8617
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8618
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8624
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8629

Mozilla Firefox

Spoločnosť Mozilla tento mesiac vo svojom prehliadači opravila dve kritické a päť závažných zraniteľností. Kritické zraniteľnosti CVE-2018-12405 a CVE-2018-12406 sa týkajú poškodenia pamäte, ktoré by mohlo vyústiť až k tomu, že by útočník mohol vzdialene vykonávať kód.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-30/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-29/

Google Chrome

Spoločnosť Google vydala tento mesiac aktualizácie, ktoré opravujú až štrnásť závažných zraniteľností.

Zdroje:
https://chromereleases.googleblog.com/2018
https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop_12.html
https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Tento mesiac bola opravená jedna kritická zraniteľnosť produktu Adobe Flash Player s označením CVE-2018-15982 na ktorú je známy aj exploit. Táto zraniteľnosť umožňuje vzdialene vykonávať kód. O tejto zraniteľnosti sa môžete dočítať viac v našom varovaní.
Okrem nej bola opravená ešte jedna závažná zraniteľnosť CVE-2018-15983, ktorá umožňuje zvýšenie práv.

V produkte Acrobat Reader bolo opravených až 38 kritických a 48 závažných zraniteľností. Spomínané zraniteľnosti sa týkajú vzdialeného vykonávania kódu, zvyšovania práv či úniku informácií.

Zraniteľné systémy:

Acrobat DC 2019.008.20081 a staršie
Acrobat Reader DC 2019.008.20081 a staršie
Acrobat 2017 2017.011.30106 a staršie
Acrobat Reader 2017 2017.011.30106 a staršie
Acrobat DC 2015 2015.006.30457 a staršie
Acrobat Reader DC 2015 2015 2015.006.30457 a staršie
Adobe Flash Player 31.0.0.153 a staršie
Adobe Flash Player Installer 31.0.0.108 a staršie

Odporúčania:

Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy nasledovne:

- Acrobat DC 2019.010.20064
- Acrobat Reader DC 2019.010.20064
- Acrobat 2017 2017.011.30110
- Acrobat Reader 2017 2017.011.30110
- Acrobat DC 2015 2015.006.30461
- Acrobat Reader DC 2015 2015.006.30461
- Adobe Flash Player 32.0.0.101
- Adobe Flash Player Installer 31.0.0.122

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/apsb18-41.html
https://helpx.adobe.com/security/products/flash-player/apsb18-42.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft tento mesiac vydala aktualizácie pre Microsoft .NET Framework opravujúce jednu kritickú zraniteľnosť. Konkrétne ide o CVE-2018-8540, ktorá umožňuje vzdialené vykonávanie kódu. Po zneužití tejto zraniteľnosti je možné prevziať kontrolu nad systémom a útočník tak má možnosť inštalovať programy; prezerať, meniť či mazať dáta; vytvárať nových používateľov s plnými právami.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8540

Oracle Java

Spoločnosť Oracle nevydala v mesiaci december žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 15. január 2019.

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

6. Iné závažné zraniteľnosti

Zraniteľnosť Kubernetes

Kritická zraniteľnosť objavená v nástroji Kubernetes umožňuje neautentifikovanému útočníkovi získať administrátorské práva ku API alebo „clustru“ v cloude. Po tom ako Kubernetes API server prijme upravenú požiadavku vyvolávajúcu chybu, je možné posielať požiadavky bez ďalšej autorizácie a to umožní vykonávať ľubovoľný kód. Ak chcete vedieť viac informácií prečítajte si naše varovanie.

Zraniteľné systémy:
Kubernetes revízie staršie ako: v1.10.11, v1.11.5, v1.12.3 alebo v1.12.0-rc.1

Odporúčania:
Aktualizácia Kubernetes aspoň na revíziu: v1.10.11, v1.11.5, v1.12.3 alebo v1.12.0-rc.1

Zraniteľnosti modulov WordPress

Boli opravené kritické zraniteľnosti troch modulov CMS systému WordPress. Tieto zraniteľnosti umožňujú zvýšenie privilégií a následne získanie prístupu do administrátorského účtu. Je takto možné získať kontrolu nad celou webstránkou. Bližšie informácie sa dozviete v našom varovaní.

Zraniteľné systémy:
- Modul WooCommerce 3.4.5 a staršie
- Modul AMP, staršie verzie ako 0.9.97.20
- Modul WP GDPR Compliance 1.4.2 a staršie

Odporúčania:
- Aktualizácia modulu WooCommerce aspoň na verziu 3.4.6 (odporúčame zapnúť automatické aktualizácie vo WordPress)
- Aktualizácia AMP aspoň na verziu 0.9.97.20
- Aktualizácia WP GDPR Compliance aspoň na verziu 1.4.3
- Odporúčame zapnúť automatické aktualizácie modulov vo WordPresse

Magellan

Bola opravená zraniteľnosť v databázovej knižnici SQLite, ktorá umožňuje útočníkom spôsobiť zlyhanie programu, čítať alokovanú pamäť či vykonávať ľubovoľný kód. Táto

zraniteľnosť zasiahla veľa aplikácií od prehliadačov postavených na platforme Chromium, cez IoT zariadenia, po Android a iOS aplikácie. Pre viac informácií si prečítajte naše varovanie.

Zraniteľné systémy:

SQLite 3.25.2 a staršie
Webové prehliadače postavené na platforme Chromium
Ďalšie aplikácie využívajúce SQLite

Odporúčania:

- Aktualizácia SQLite aspoň na verziu 3.26.0
- Aktualizácia aplikácií využívajúcich SQLite na najnovšiu verziu (napr. verzie webových prehliadačov postavených na platforme Chromium, ktoré využívajú aspoň Chromium 71.0.3578.80)
- Nepoužívať aplikácie, ktoré nemajú aktualizovanú súčasť SQLite

Zraniteľnosť WordPress

Tento mesiac sa opravilo sedem závažných zraniteľností vo verziách WordPress 4.x a 5.0. Niektoré z týchto zraniteľností môžu viesť až k prevzatiu kontroly nad webstránkou. Viac informácii nájdete v našom varovaní.

Zraniteľné systémy:

WordPress verzie 4.x
WordPress 5.0

Odporúčania:

- Aktualizácia WordPress 4 aspoň na verziu 4.9.9
- Aktualizácia WordPress 5 aspoň na verziu 5.0.1