Mesačný prehľad kritických zraniteľností
November 2018

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft tento mesiac opravila tri kritické zraniteľnosti týkajúce sa operačného systému Windows. Každá z týchto zraniteľností umožňuje útočníkovi vzdialene vykonávať kód.

Jedná s o zraniteľnosti CVE-2018-8476, CVE-2018-8544 a CVE-2018-8553. Prvá z nich nastáva kvôli tomu, že Windows Deployment Services TFTP Server nesprávne narába s objektmi v pamäti. Po zneužití tejto zraniteľnosti má útočník možnosť vykonávať kód so zvýšenými právami. Zneužiť ju je možné pomocou špeciálne upravenej požiadavky. Druhá spomínaná zraniteľnosť existuje vďaka nesprávnemu narábaniu VBScript engine s objektmi v pamäti. Zraniteľnosť môže poškodiť pamäť takým spôsobom, že dovolí útočníkovi vykonávať kód ako práve prihlásený používateľ. Ak je používateľ prihlásený ako administrátor tak umožní útočníkovi prevziať kontrolu nad systémom, mohol by inštalovať programy; prezerať, meniť či mazať dáta; vytvárať nových používateľov s plnými právami. Útočník na zneužitie môže použiť špeciálne pripravenú stránku, musí však presvedčiť používateľa aby ju navštívil. Je taktiež možné pridať prvok ActiveX označený ako bezpečný na inicializáciu do dokumentu Microsoft Office. Posledná spomínaná kritická zraniteľnosť nastáva nesprávnym narábaním Microsoft Graphics Components s objektmi v pamäti. Po zneužití môže útočník vykonávať kód na systéme. Na zneužitie je potrebné aby používateľ otvoril špeciálne pripravený súbor.

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 1803 for 32-bit Systems
Windows 10 Version 1803 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 2019
Windows Server 2019 (Server Core installation)
Windows Server, version 1709 (Server Core installation)
Windows Server, version 1803 (Server Core installation)

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-2018-8476
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8544
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8553

2. Kancelárske balíky Microsoft Office a Office Web Apps

V balíkoch Microsoft Office bolo tento mesiac opravených štrnásť závažných zraniteľností.
Dve zraniteľnosti CVE-2018-8568, CVE-2018-8572 umožňujú zvýšenie práv. Obidve sa týkajú Microsoft SharePoint servera pričom umožňujú 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-2018-8522, CVE-2018-8524, CVE-2018-8539, CVE-2018-8573, CVE-2018-8574, CVE-2018-8575, CVE-20188576 a CVE-2018-8577 sú spôsobené tým, že Microsoft Excel, Microsoft Word, Microsoft Projet alebo Microsoft Outlook nesprávne narábajú s objektmi v pamäti. Ďalšia zraniteľnosť rovnakého druhu, CVE-2018-8582, súvisí so spôsobom, ako Microsoft Outlook analyzuje špeciálne upravené súbory na export pravidiel. Na zneužitie je možné použiť špeciálne pripravený súbor. Útočník musí ešte presvedčiť používateľa, aby tento 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-2018-8578, CVE-2018-8579 a CVE-2018-8558 spôsobujú únik informácií. Prvá sa týka Microsoft SharePoint Servera, ktorý nesprávne zverejňuje svoju štruktúru

priečinkov pri vykresľovaní stránok. Útočník po zneužití môže vidieť cestu k skriptom načítaným na stránke. Na zneužitie musí mať útočník prístup k špecifickej SharePoint stránke, ktorá je postihnutá touto zraniteľnosťou. Druhé dve spomínané zraniteľnosti sa týkajú programu Microsoft Outlook. Jedna umožňuje používateľom zdieľať pripojené súbory tak aby boli prístupné aj anonymnému užívateľovi. Na zneužitie je potrebné poslať prílohu ako link na email. Druhá nastáva, keď Microsoft Outlook nerešpektuje prednastavený typ odkazu nakonfigurovaný cez SharePoint Online Admin Center.

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 Outlook 2019 (32-bitová verzia)
Microsoft Outlook 2019 (64-bitová verzia)
Microsoft Word 2010 Service Pack 2 (32-bitová verzia)
Microsoft Word 2010 Service Pack 2 (64-bitová verzia)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bitová verzia)
Microsoft Word 2013 Service Pack 1 (64-bitová verzia)
Microsoft Word 2016 (32-bitová verzia)
Microsoft Word 2016 (64-bitová verzia)
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office Web Apps 2013 Service Pack 1
Microsoft Office 2010 Service Pack 2 (32-bitová verzia)
Microsoft Office 2010 Service Pack 2 (64-bitová verzia)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bitová verzia)
Microsoft Office 2013 Service Pack 1 (64-bitová verzia)
Microsoft Office 2016 (32-bitová verzia)
Microsoft Office 2016 (64-bitová verzia)

Microsoft Office 2016 pre Mac
Microsoft Office 2019 (32-bitová verzia)
Microsoft Office 2019 (64-bitová verzia)
Microsoft Office 2019 pre Mac
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
Microsoft Project 2013 Service Pack 1 (32-bitová verzia)
Microsoft Project 2013 Service Pack 1 (64-bitová verzia)
Microsoft Project 2016 (32-bitová verzia)
Microsoft Project 2016 (64-bitová verzia)
Microsoft Project Server 2013 Service Pack 1 (32-bitová verzia)
Microsoft Project Server 2013 Service Pack 1 (64-bitová verzia)

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-2018-8572
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8568
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8578
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8579
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8558
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8582
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8577
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8576
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8575
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8574
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8573
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8539
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8524
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8522

3. Internetové prehliadače

Microsoft Internet Explorer

Iba dve kritické zraniteľnosti boli opravené tento mesiac v prehliadači Internet Explorer. Zraniteľnosti spôsobujúce poškodenie pamäte môžete nájsť pod označeniami: CVE-2018-8552 a CVE-2018-8570. Zraniteľnosti sú spôsobené nesprávnym narábaním prehliadača Internet Explorer s objektmi v pamäti. Môžu 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 zneužitie týchto zraniteľností musí útočník presvedčiť používateľa aby navštívil špeciálne vytvorenú stránku, ktorej odkaz môže poslať napríklad pomocou emailu alebo rýchlej správy.

Zraniteľné systémy:

Microsoft Internet Explorer verzie 9, 10, 11

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-2018-8552
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8570

Microsoft Edge

Osem kritických zraniteľností bolo opravených tento mesiac v prehliadači Microsoft Edge, pričom zneužitie týchto zraniteľností môže poškodiť pamäť. Opravenými zraniteľnosťami sú: CVE-2018-8541, CVE-2018-8542, CVE-2018-8543, CVE-2018-8551, CVE-2018-8555, CVE-2018-8556, CVE-2018-8557 a CVE-2018-8588. 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 aj 64-bitových verziách
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-2018-8541
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8542
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8543
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8551
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8555
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8556
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8557
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8588

Mozilla Firefox

Spoločnosť Mozilla tento mesiac neopravila žiadne kritické alebo závažné zraniteľnosti.

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

Google Chrome

Spoločnosť Google vydala tento mesiac aktualizácie, ktoré opravujú iba jednu závažnú zraniteľnosť označenú ako CVE-2018-17479.

Zdroje:
https://chromereleases.googleblog.com/2018
https://chromereleases.googleblog.com/2018/11/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Jedna závažná zraniteľnosť produktu Adobe Acrobat Reader, na ktorú je známy aj proof-of-concept bola opravená tento mesiac spoločnosťou Adobe. Zraniteľnosť má označenie CVE-2018-15979 a môže spôsobiť únik zahashovaného hesla používateľa. Spoločnosť Adobe opravila taktiež jednu závažnú zraniteľnosť CVE-2018-15978 týkajúcu sa úniku informácií v produkte Adobe Flash Player. V produkte Adobe Flash Player bola opravená taktiež zraniteľnosť označená ako CVE-2018-15981, ktorá umožňuje útočníkovi vzdialene vykonávať kód. Viac o tejto zraniteľnosti sa môžete dočítať v našom varovaní.

Zraniteľné systémy:
Acrobat DC 2019.008.20080 a staršie
Acrobat Reader DC 2019.008.20080 a staršie
Acrobat 2017 2017.011.30105 a staršie
Acrobat Reader 2017 2017.011.30105 a staršie
Acrobat DC 2015 2015.006.30456 a staršie
Acrobat Reader DC 2015 2015 2015.006.30456 a staršie
Adobe Flash Player 31.0.0.122 a staršie

Odporúčania:
Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy nasledovne:

- Acrobat DC 2019.008.20081
- Acrobat Reader DC 2019.008.20081
- Acrobat 2017 2017.011.30106
- Acrobat Reader 2017 2017.011.30106
- Acrobat DC 2015 2015.006.30457
- Acrobat Reader DC 2015 2015.006.30457
- Adobe Flash Player 31.0.0.148

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

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb18-40.html
https://helpx.adobe.com/security/products/flash-player/apsb18-39.html

5. Frameworky

Microsoft .NET Framework

Tento mesiac spoločnosť Microsoft nevydala žiadne aktualizácie pre Microsoft .NET Framework.

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

Oracle Java

Spoločnosť Oracle nevydala v mesiaci november 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

Zraniteľnosti BleedingBit

Dve zraniteľnosti nazvané BleedingBit sa týkajú Bluetooth Low Energy (BLE) čipov od spoločnosti Texas Instruments a umožňujú prevzatie kontroly nad zraniteľným zariadením bez autentifikácie a prienik do siete v ktorej je pripojené. Pre viac informácií si prečítajte naše varovanie.

Zraniteľné systémy:

- *CVE-2018-16986:* Čipy Texas Instuments CC2640 a CC2650 s firmvérom BLE-STACK 2.2.1 a starším a CC2640R2 s firmvérom BLE-STACK 1.0 a starším, ktoré sa používajú vo wi-fi prístupových bodoch od Cisco a Meraki. Podľa spoločnosti Armis sú zneužiteľné prístupové body 1542 AP, 1815 AP, 4800 AP, MR33, MR30H, MR74, and

MR53E. Cisco dodáva, že zraniteľné sú série prístupových bodov Aironet 1800i, 1810, 1815i, 1815m, 1815w, 4800, 1540 a Meraki MR30H AP, MR33 AP, MR42E AP, MR53E AP, MR74.

- *CVE-2018-7080:* Čipy Texas Instuments CC2642R2, CC2640R2, CC2640, CC2650, CC2540, a CC2541, ktoré sa používajú vo wi-fi prístupových bodoch Aruba série 300. Cisco: firmvér prístupových bodov Aironet od verzie 8.7 po verziu pred 8.8.100; firmvér pre zariadenia Meraki verzie staršej ako MR 25.13

Odporúčania:

- *CVE-2018-16986:* aktualizácia firmvéru BLE-STACK aspoň na verziu 2.2.2
- *CVE-2018-7080:* vypnutie funkcie OAD (je určená len na testovacie účely)
- *Cisco:* aktualizácia firmvéru pre zariadenia Aironet aspoň na verziu 8.8.100; aktualizácia firmvéru pre zariadenia Meraki aspoň na verziu MR 25.13

Zraniteľnosti modulov WordPress

Boli opravené kritické zraniteľnosti troch modulov CMS systému WordPress. Tieto zraniteľnosti umožňujú zvýšenie privilégií a následne získanie prístupu do administrátorského účtu. Takto je 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
- Mobul 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

Zraniteľnosť PHP

Zraniteľnosť PHP funkcie Imap_open umožňuje ovládnuť server tým, že pri nesprávnom kontrolovaní vstupov dokáže spúšťať shell príkazy na vzdialenom serveri. Pre viac informácií si prečítajte naše varovanie.

Zraniteľné systémy:

PHP, funkcia Imap_open

Odporúčania:

- Ak server využíva funkciu imap_open jazyka PHP a vstup do premennej "string $mailbox" kontroluje používateľ, server musí vykonávať kontrolu tohto vstupu
- Aktualizácia v čase písania tohto varovania nebola dostupná

Zero-day zraniteľnosť vo VirtualBox

Objavená zraniteľnosť umožňuje preniknúť z virtuálneho systému do hosťovského a následne využitím ďalších metód eskalovať privilégiá až na úroveň systému. Viac informácií môžete nájsť v našom varovaní.

Zraniteľné systémy:

VirtualBox (virtuálna sieťová karta Intel PRO/1000 MT Desktop (82540EM) v prednastavenom sieťovom móde NAT) pre všetky podporované OS

Odporúčania:

- Do vydania aktualizácie používať inú virtuálnu sieťovú kartu ako Intel PRO/1000 MT Desktop (82540EM)
- Prípadne využívať iný mód ako NAT